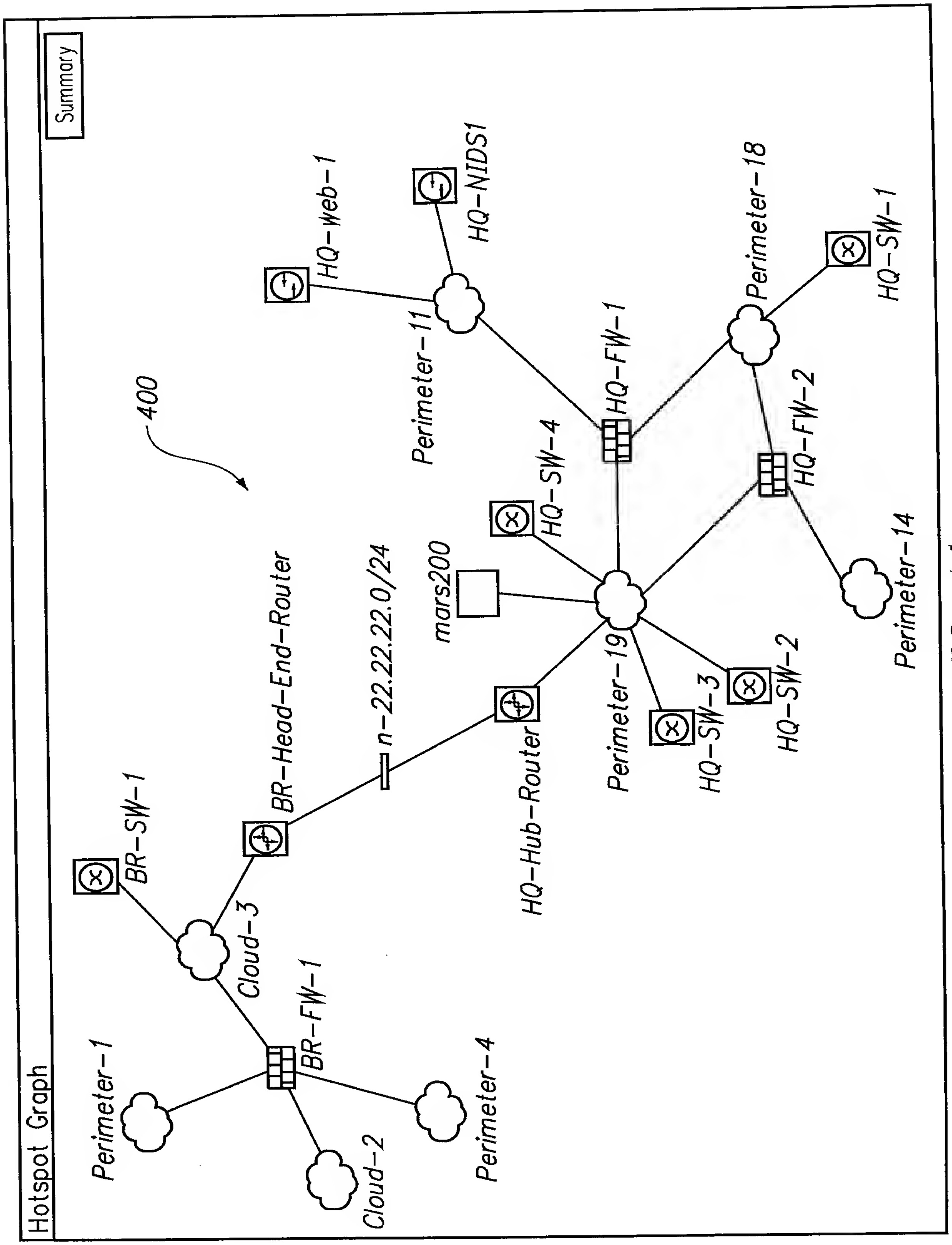

Hotspot Graph
Summary
400
Perimeter-1
Cloud-2
Perimeter-4
BR-FW-1
Cloud-3
BR-SW-1
BR-Head-End-Router
n-22.22.22.0/24
HQ-Hub-Router
mars200
Perimeter-19
HQ-SW-3
HQ-SW-2
HQ-SW-4
HQ-FW-1
HQ-FW-2
Perimeter-14
Perimeter-11
HQ-web-1
HQ-NIDS1
Perimeter-18
HQ-SW-1

FIG. 4A

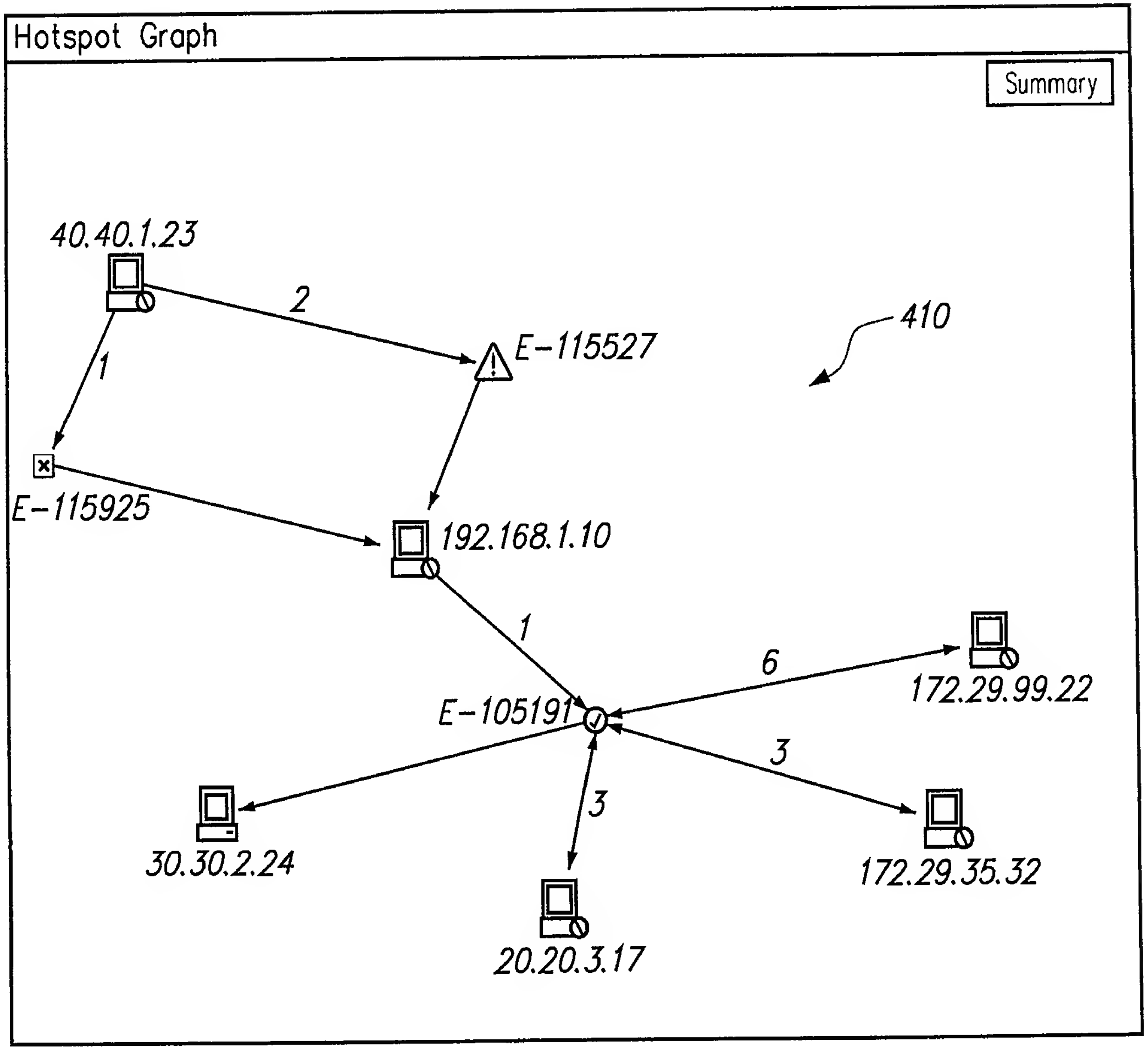

Hotspot Graph
Summary
410
40.40.1.23
2
1
E-115527
E-115925
192.168.1.10
1
6
172.29.99.22
E-105191
3
3
30.30.2.24
20.20.3.17
172.29.35.32

FIG. 4B

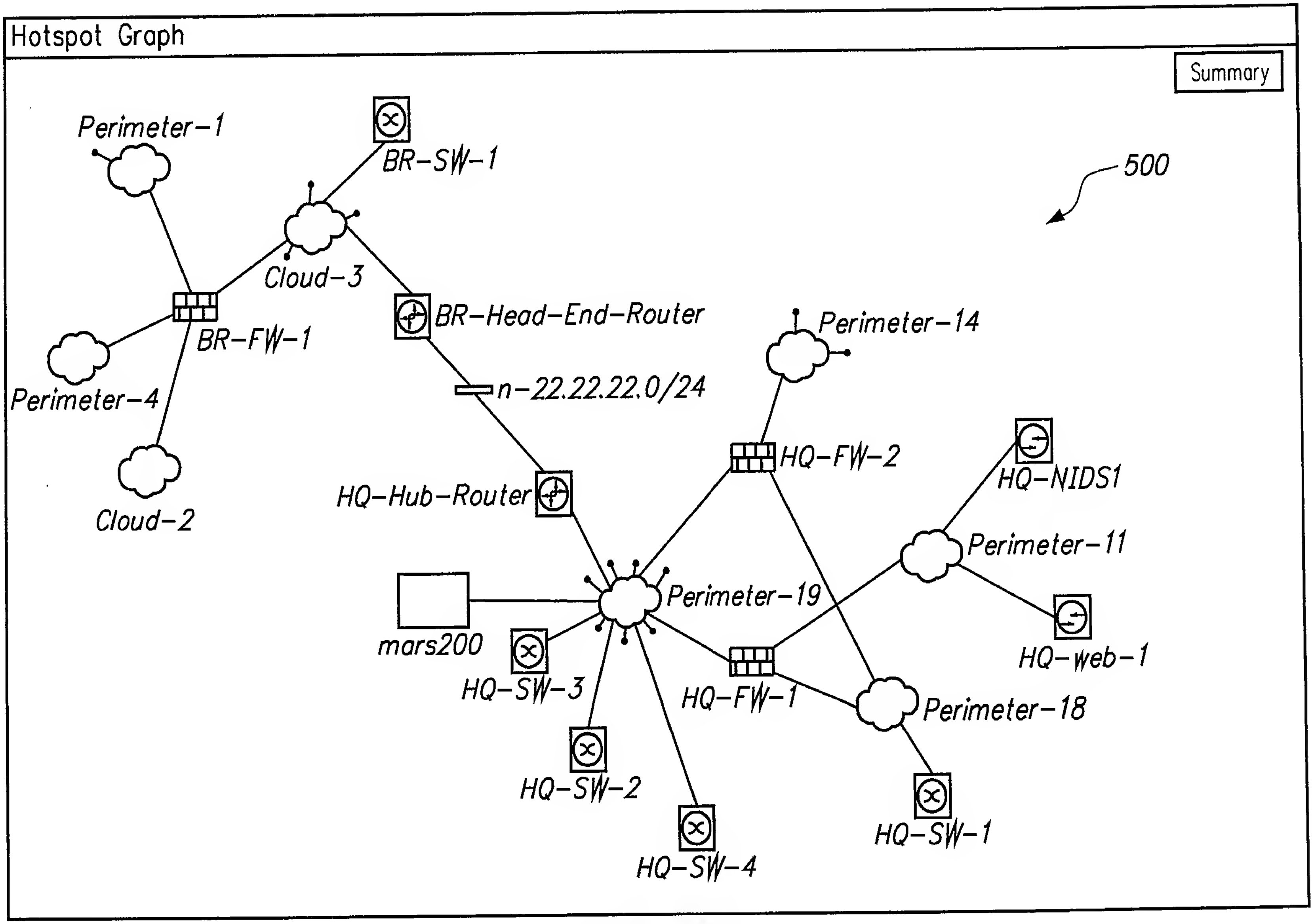
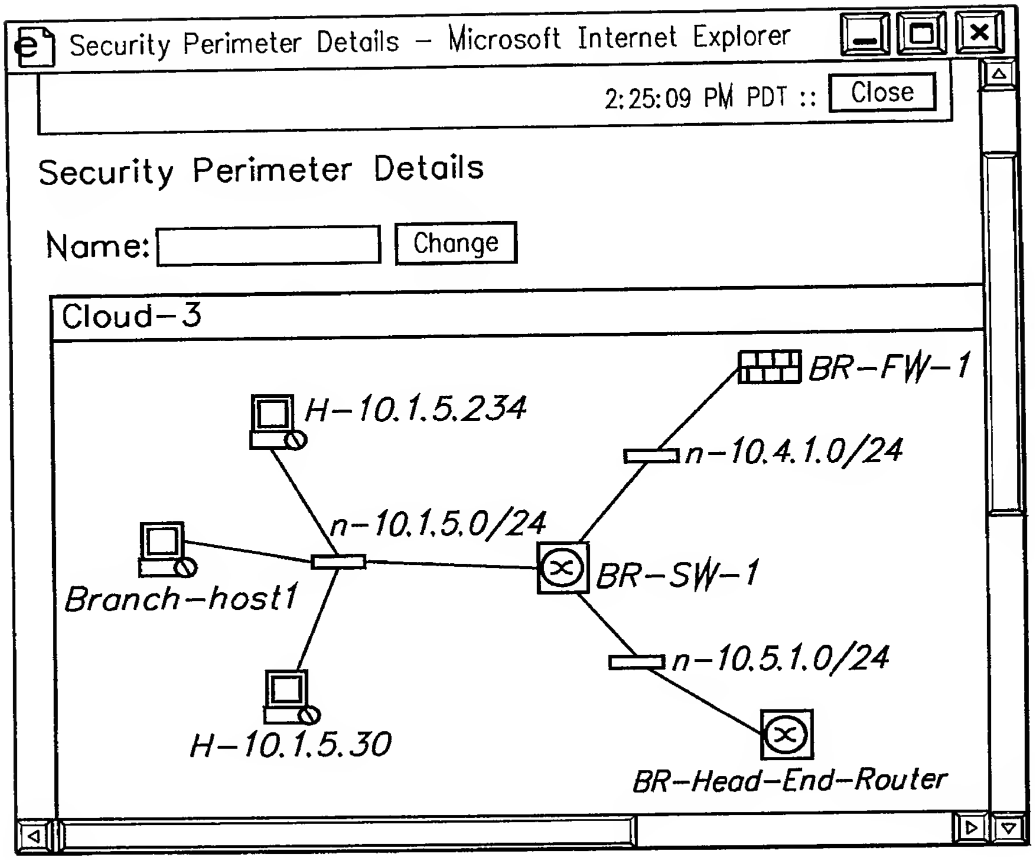
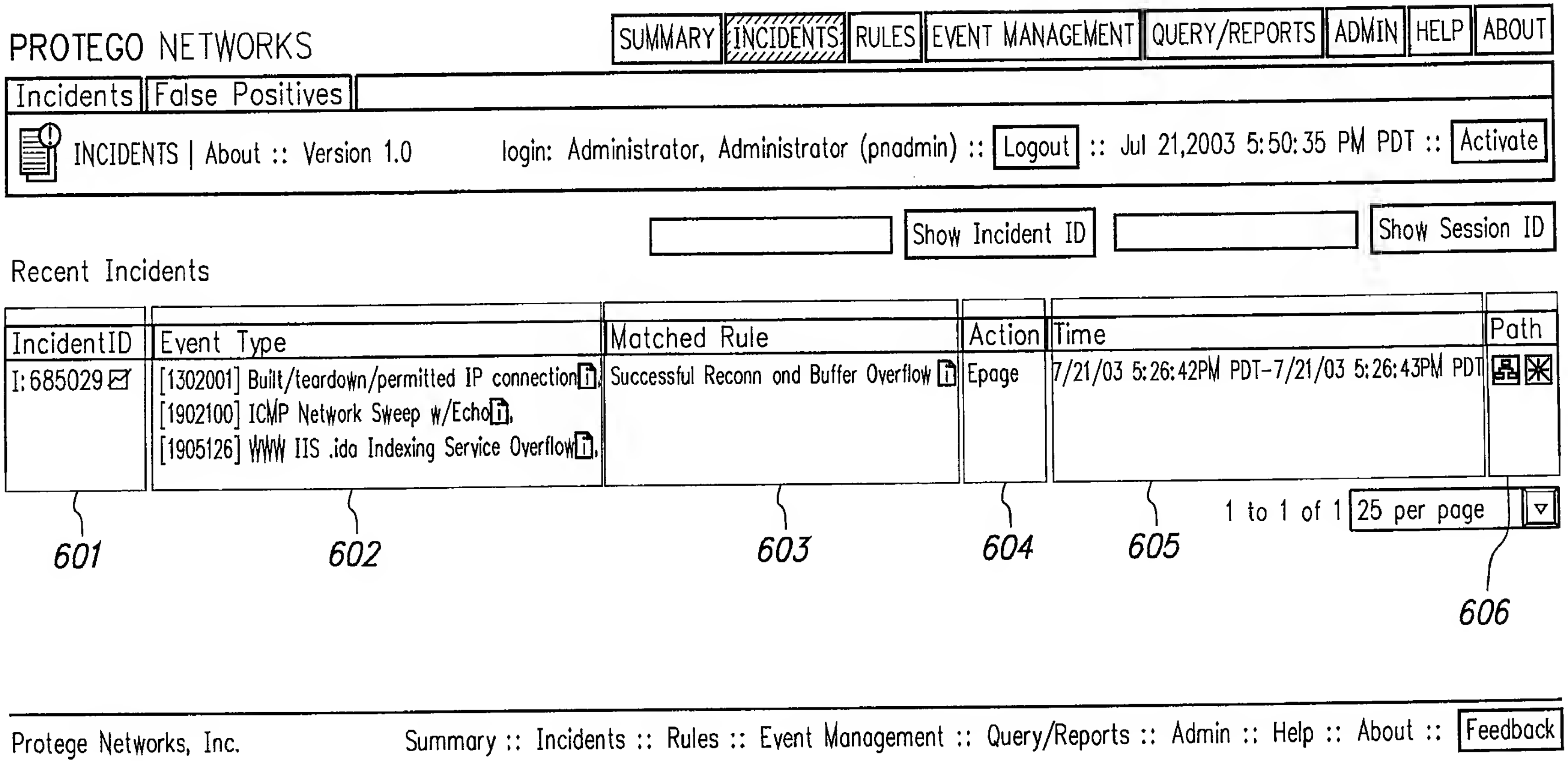

Hotspot Graph
Summary
500
Perimeter-1
BR-SW-1
Cloud-3
BR-FW-1
Perimeter-4
Cloud-2
BR-Head-End-Router
n-22.22.22.0/24
Perimeter-14
HQ-FW-2
HQ-NIDS1
HQ-Hub-Router
Perimeter-11
Perimeter-19
mars200
HQ-web-1
HQ-SW-3
HQ-FW-1
Perimeter-18
HQ-SW-2
HQ-SW-1
HQ-SW-4

FIG. 5A



Security Perimeter Details – Microsoft Internet Explorer
2:25:09 PM PDT ::
Close
Security Perimeter Details
Name:
Change
Cloud-3
BR-FW-1
H-10.1.5.234
n-10.4.1.0/24
n-10.1.5.0/24
Branch-host1
BR-SW-1
n-10.5.1.0/24
H-10.1.5.30
BR-Head-End-Router

FIG. 5B



INCIDENTS | About :: Version 1.0 login: Administrator, Administrator (pnadmin) :: Logout :: Jul 21,2003 5:50:35 PM PDT :: Activate

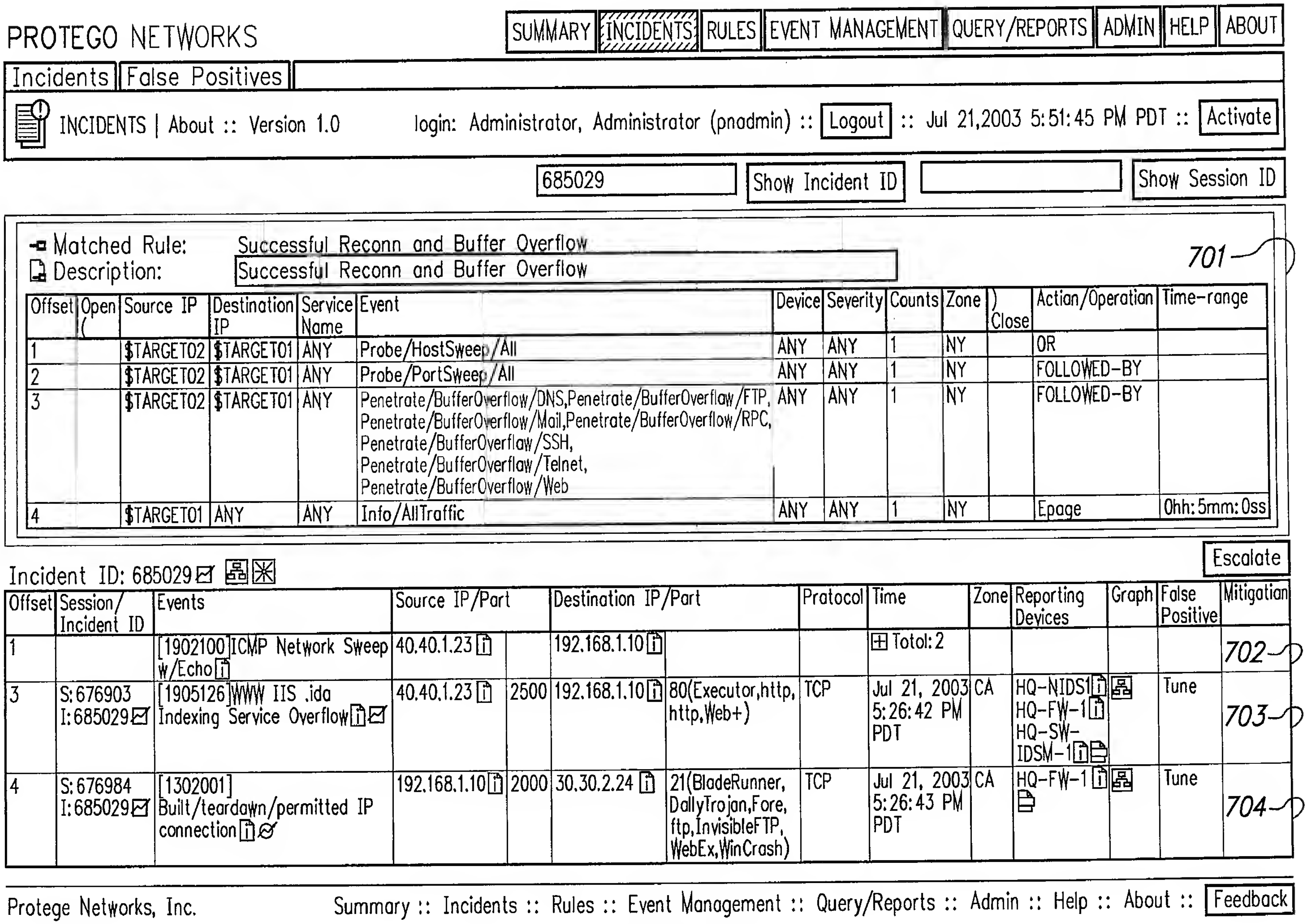
Recent Incidents

| IncidentID | Event Type | Matched Rule | Action | Time | Path |
|---|---|---|---|---|---|
| I:685029 | [1302001] Built/teardown/permitted IP connection,<br>[1902100] ICMP Network Sweep w/Echo,<br>[1905126] WWW IIS .ida Indexing Service Overflow, | Successful Reconn and Buffer Overflow | Epage | 7/21/03 5:26:42PM PDT-7/21/03 5:26:43PM PDT | |

1 to 1 of 1

Protege Networks, Inc. Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 6



PROTEGO NETWORKS

SUMMARY | INCIDENTS | RULES | EVENT MANAGEMENT | QUERY/REPORTS | ADMIN | HELP | ABOUT

Incidents | False Positives

INCIDENTS | About :: Version 1.0   login: Administrator, Administrator (pnadmin) :: Logout :: Jul 21,2003 5:51:45 PM PDT :: Activate

685029 | Show Incident ID | | Show Session ID

Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

| Offset | Open ( | Source IP | Destination IP | Service Name | Event | Device | Severity | Counts | Zone | ) Close | Action/Operation | Time-range |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | $TARGET02 | $TARGET01 | ANY | Probe/HostSweep/All | ANY | ANY | 1 | NY | | OR | |
| 2 | | $TARGET02 | $TARGET01 | ANY | Probe/PortSweep/All | ANY | ANY | 1 | NY | | FOLLOWED-BY | |
| 3 | | $TARGET02 | $TARGET01 | ANY | Penetrate/BufferOverflow/DNS,Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail,Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web | ANY | ANY | 1 | NY | | FOLLOWED-BY | |
| 4 | | $TARGET01 | ANY | ANY | Info/AllTraffic | ANY | ANY | 1 | NY | | Epage | 0hh:5mm:0ss |

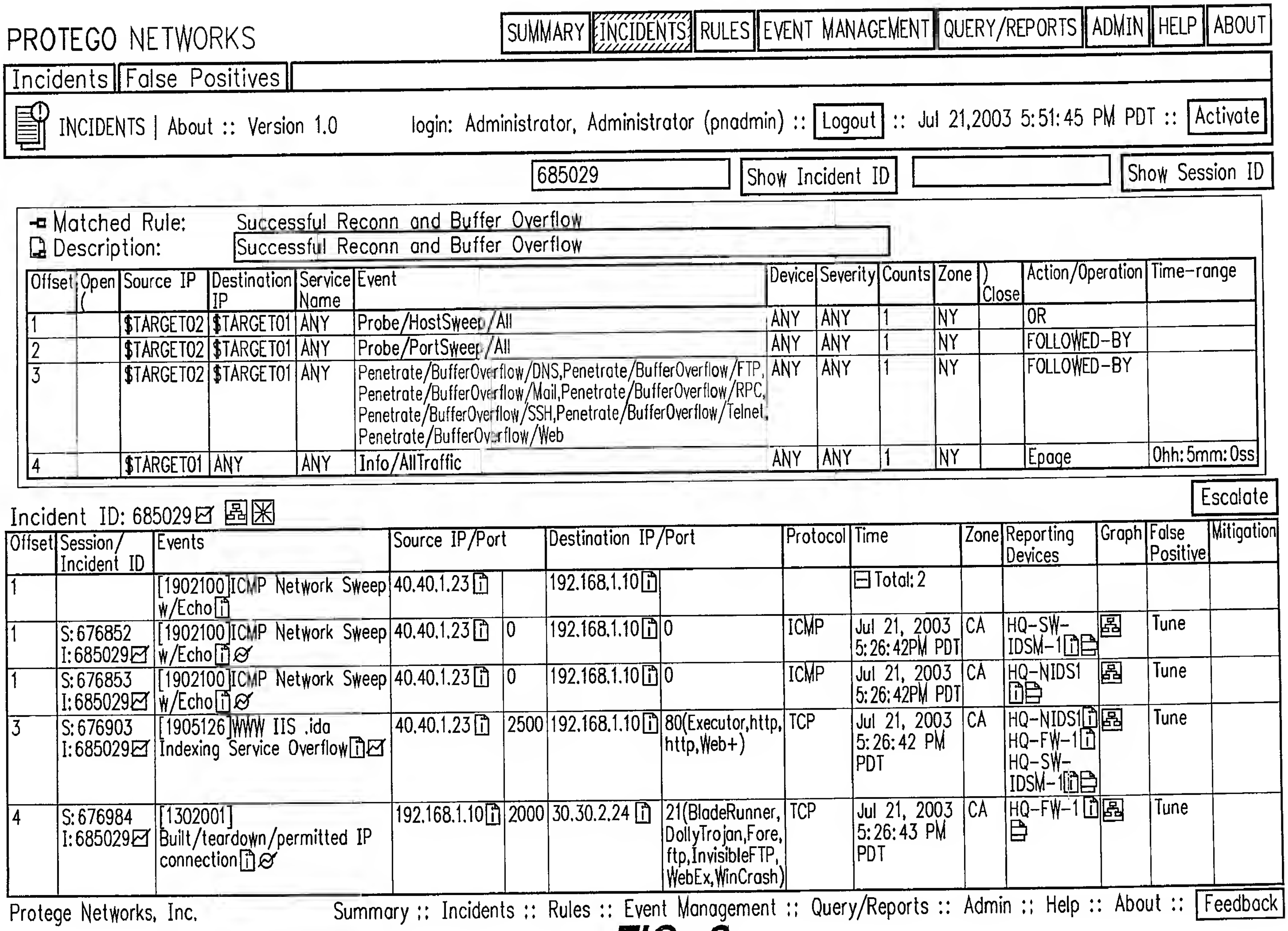
Escalate

Incident ID: 685029☑

| Offset | Session/ Incident ID | Events | Source IP/Part | | Destination IP/Part | | Pratocol | Time | Zone | Reporting Devices | Graph | False Positive | Mitigation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | [1902100]ICMP Network Sweep w/Echo | 40.40.1.23 | | 192.168.1.10 | | | ⊞ Totol:2 | | | | | |
| 3 | S:676903<br>I:685029☑ | [1905126]WWW IIS .ida Indexing Service Overflow☑ | 40.40.1.23 | 2500 | 192.168.1.10 | 80(Executor,http, http,Web+) | TCP | Jul 21, 2003 5:26:42 PM PDT | CA | HQ-NIDS1<br>HQ-FW-1<br>HQ-SW-IDSM-1 | | Tune | |
| 4 | S:676984<br>I:685029☑ | [1302001] Built/teardown/permitted IP connection | 192.168.1.10 | 2000 | 30.30.2.24 | 21(BladeRunner, DallyTrojan,Fore, ftp,InvisibleFTP, WebEx,WinCrash) | TCP | Jul 21, 2003 5:26:43 PM PDT | CA | HQ-FW-1 | | Tune | |

Protege Networks, Inc.   Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 7



Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

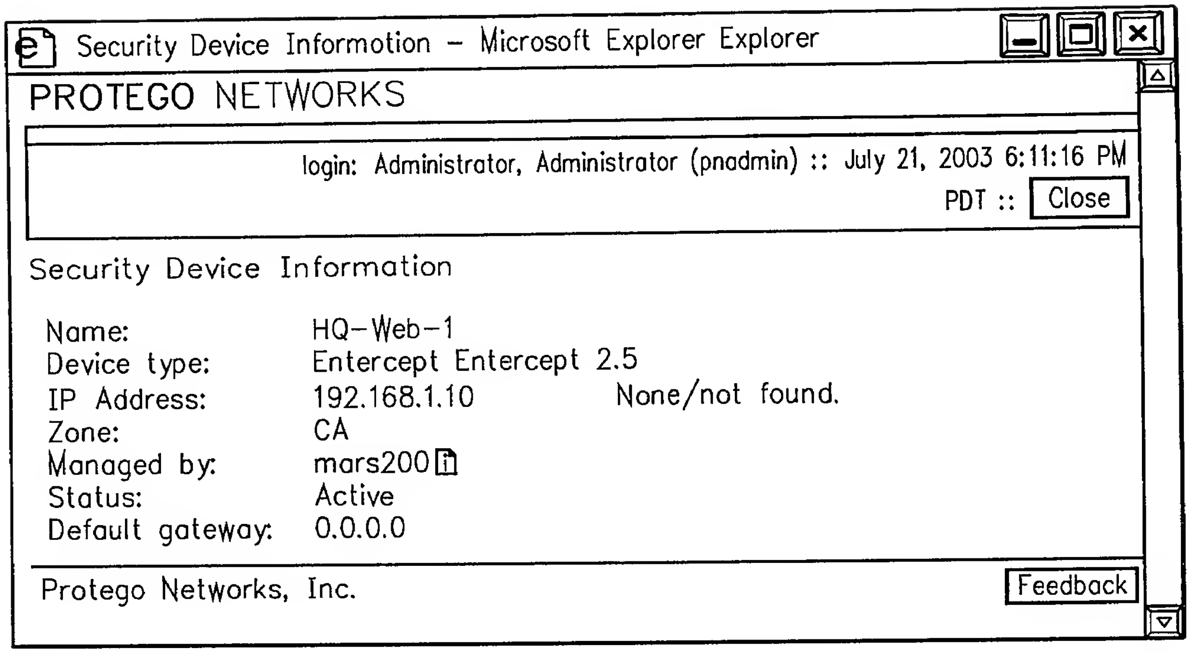
| Offset | Open ( | Source IP | Destination IP | Service Name | Event | Device | Severity | Counts | Zone | ) Close | Action/Operation | Time-range |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | $TARGET02 | $TARGET01 | ANY | Probe/HostSweep/All | ANY | ANY | 1 | NY | | OR | |
| 2 | | $TARGET02 | $TARGET01 | ANY | Probe/PortSweep/All | ANY | ANY | 1 | NY | | FOLLOWED-BY | |
| 3 | | $TARGET02 | $TARGET01 | ANY | Penetrate/BufferOverflow/DNS,Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail,Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH,Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web | ANY | ANY | 1 | NY | | FOLLOWED-BY | |
| 4 | | $TARGET01 | ANY | ANY | Info/AllTraffic | ANY | ANY | 1 | NY | | Epage | 0hh:5mm:0ss |

Incident ID: 685029

| Offset | Session/ Incident ID | Events | Source IP/Port | | Destination IP/Port | | Protocol | Time | Zone | Reporting Devices | Graph | False Positive | Mitigation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | [1902100]ICMP Network Sweep w/Echo | 40.40.1.23 | | 192.168.1.10 | | | ⊟ Total: 2 | | | | | |
| 1 | S:676852<br>I:685029 | [1902100]ICMP Network Sweep w/Echo | 40.40.1.23 | 0 | 192.168.1.10 | 0 | ICMP | Jul 21, 2003 5:26:42PM PDT | CA | HQ-SW-IDSM-1 | | Tune | |
| 1 | S:676853<br>I:685029 | [1902100]ICMP Network Sweep w/Echo | 40.40.1.23 | 0 | 192.168.1.10 | 0 | ICMP | Jul 21, 2003 5:26:42PM PDT | CA | HQ-NIDS1 | | Tune | |
| 3 | S:676903<br>I:685029 | [1905126]WWW IIS .ida Indexing Service Overflow | 40.40.1.23 | 2500 | 192.168.1.10 | 80(Executor,http, http,Web+) | TCP | Jul 21, 2003 5:26:42 PM PDT | CA | HQ-NIDS1<br>HQ-FW-1<br>HQ-SW-IDSM-1 | | Tune | |
| 4 | S:676984<br>I:685029 | [1302001] Built/teardown/permitted IP connection | 192.168.1.10 | 2000 | 30.30.2.24 | 21(BladeRunner, DollyTrojan,Fore, ftp,InvisibleFTP, WebEx,WinCrash) | TCP | Jul 21, 2003 5:26:43 PM PDT | CA | HQ-FW-1 | | Tune | |

Protege Networks, Inc. Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About ::

FIG. 8



PROTEGO NETWORKS

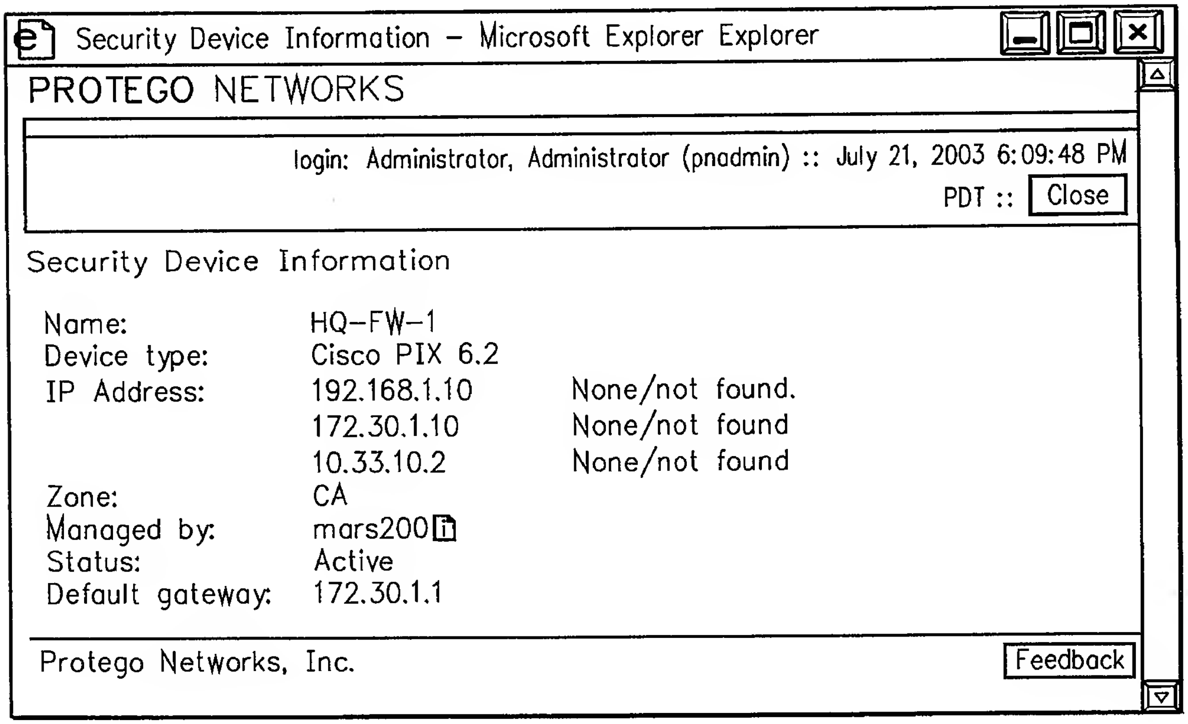
login: Administrator, Administrator (pnadmin) :: July 21, 2003 6:11:16 PM PDT ::

Security Device Information

| | | |
|---|---|---|
| Name: | HQ-Web-1 | |
| Device type: | Entercept Entercept 2.5 | |
| IP Address: | 192.168.1.10 | None/not found. |
| Zone: | CA | |
| Managed by: | mars200 🗎 | |
| Status: | Active | |
| Default gateway: | 0.0.0.0 | |

Protego Networks, Inc.

FIG. 9



PROTEGO NETWORKS

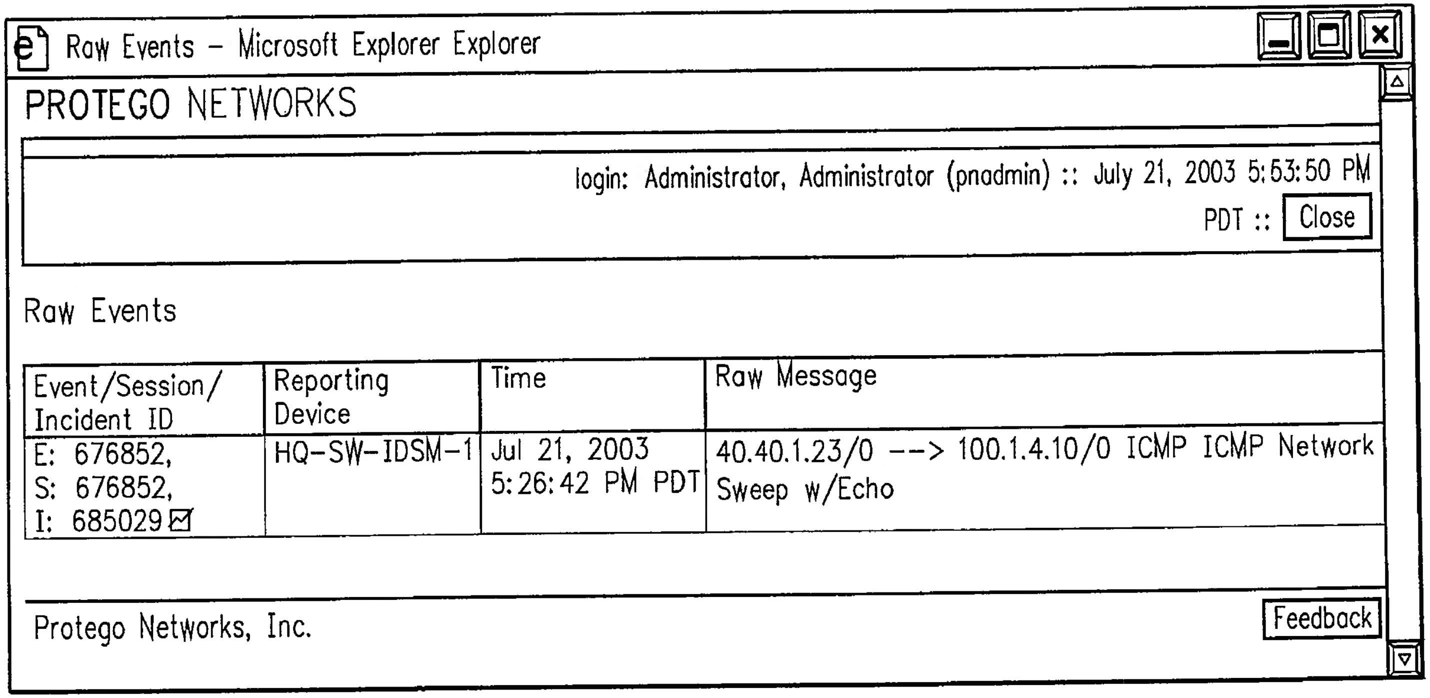
login: Administrator, Administrator (pnadmin) :: July 21, 2003 6:09:48 PM PDT ::

Security Device Information

| | | |
|---|---|---|
| Name: | HQ-FW-1 | |
| Device type: | Cisco PIX 6.2 | |
| IP Address: | 192.168.1.10 | None/not found. |
| | 172.30.1.10 | None/not found |
| | 10.33.10.2 | None/not found |
| Zone: | CA | |
| Managed by: | mars200 🗎 | |
| Status: | Active | |
| Default gateway: | 172.30.1.1 | |

Protego Networks, Inc.

FIG. 10

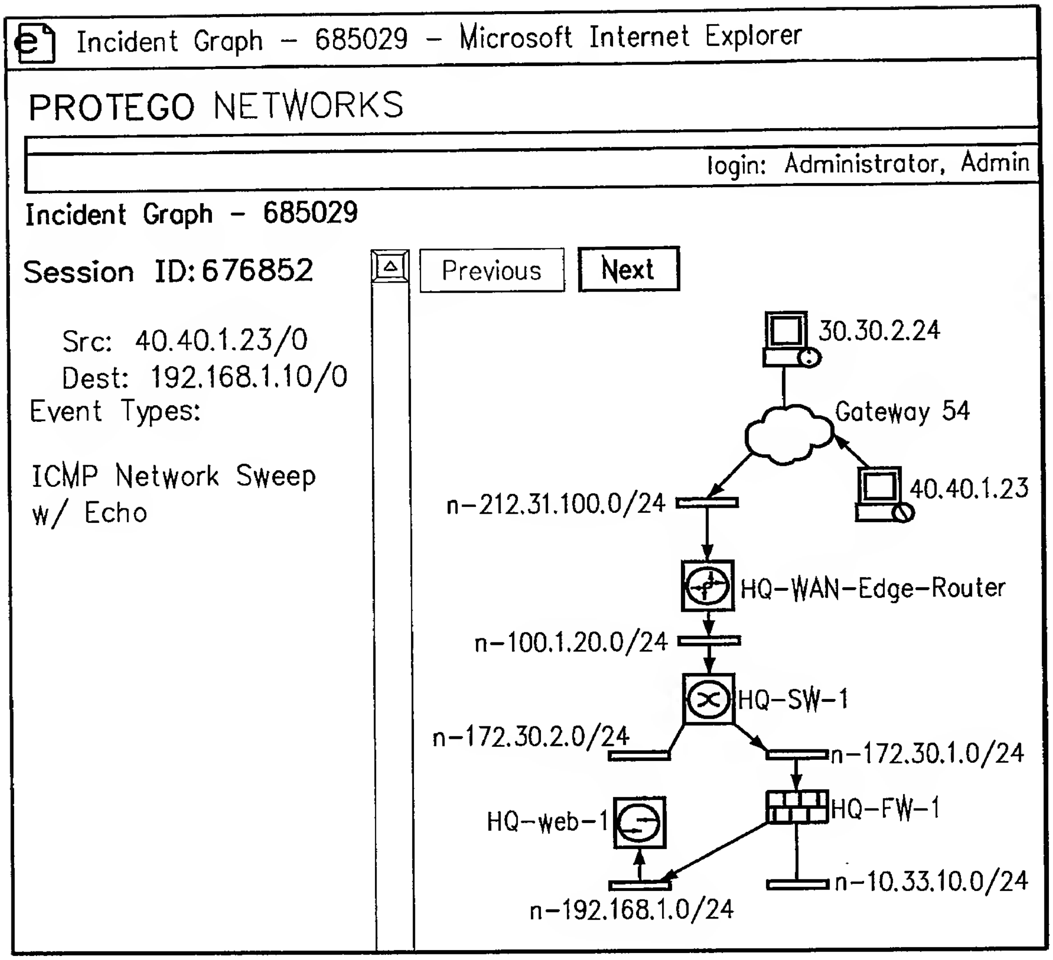


login: Administrator, Administrator (pnadmin) :: July 21, 2003 5:53:50 PM PDT :: Close

Raw Events

| Event/Session/ Incident ID | Reporting Device | Time | Raw Message |
|---|---|---|---|
| E: 676852,<br>S: 676852,<br>I: 685029 ☑ | HQ-SW-IDSM-1 | Jul 21, 2003 5:26:42 PM PDT | 40.40.1.23/0 --> 100.1.4.10/0 ICMP ICMP Network Sweep w/Echo |

FIG. 11A



Incident Graph – 685029 – Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Admin

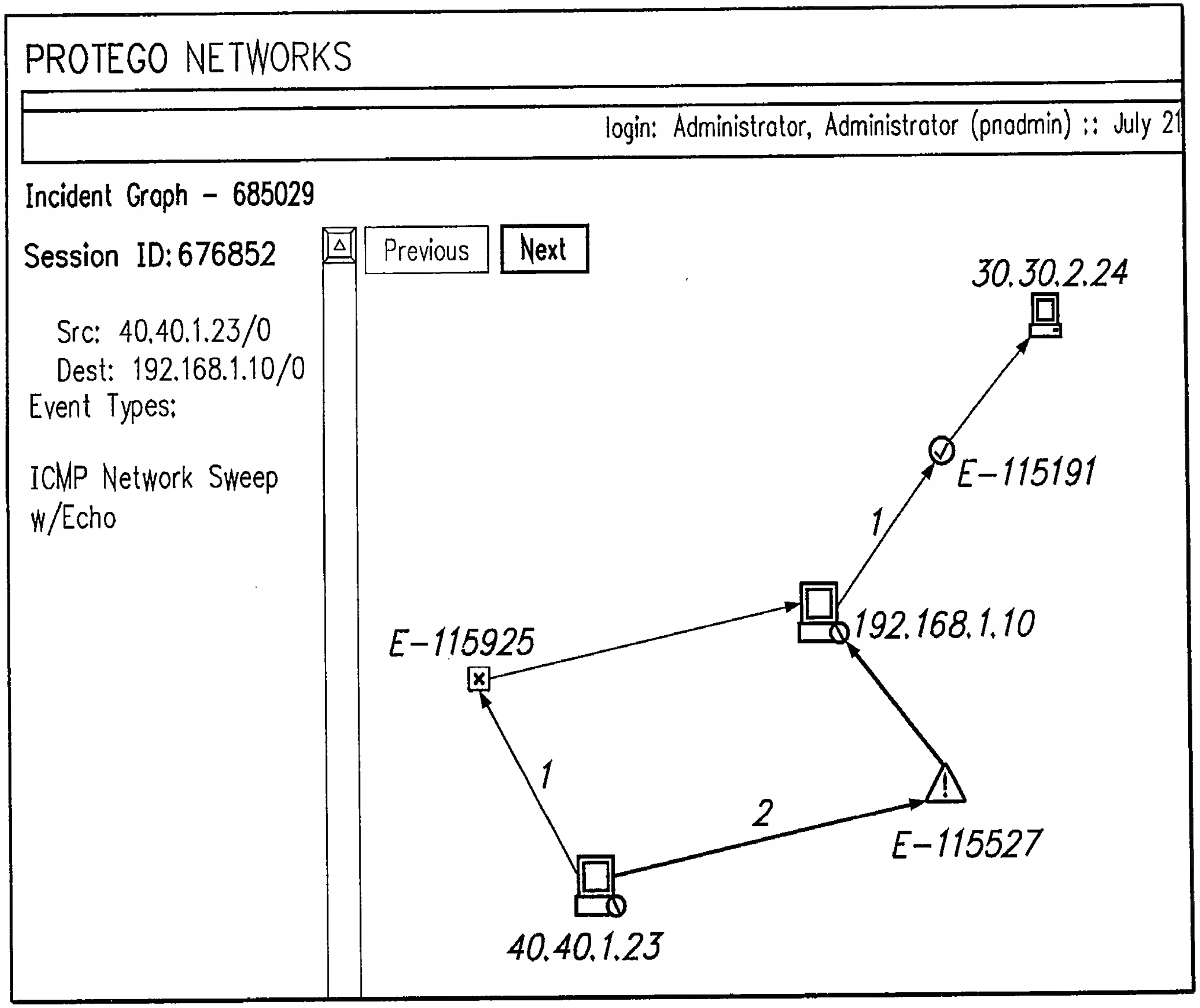
Incident Graph - 685029

Session ID: 676852

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep
w/ Echo

FIG. 11B



PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: July 21

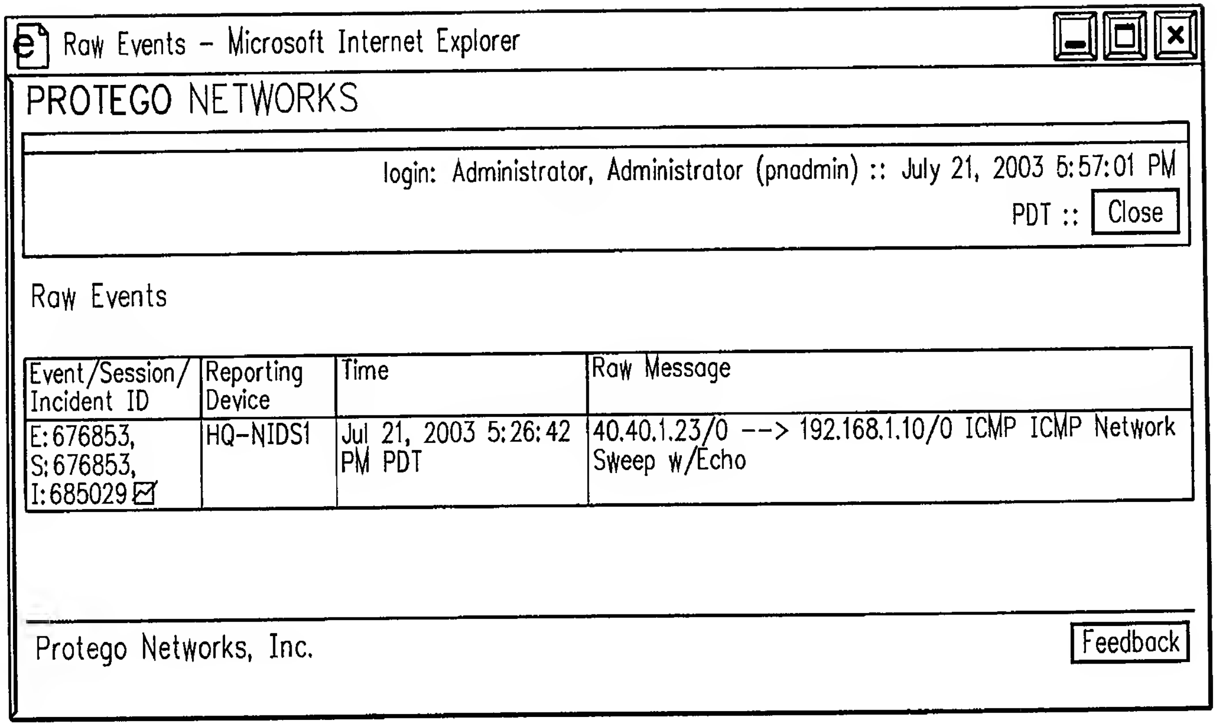
Incident Graph - 685029

Session ID: 676852

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep
w/Echo

FIG. 11C



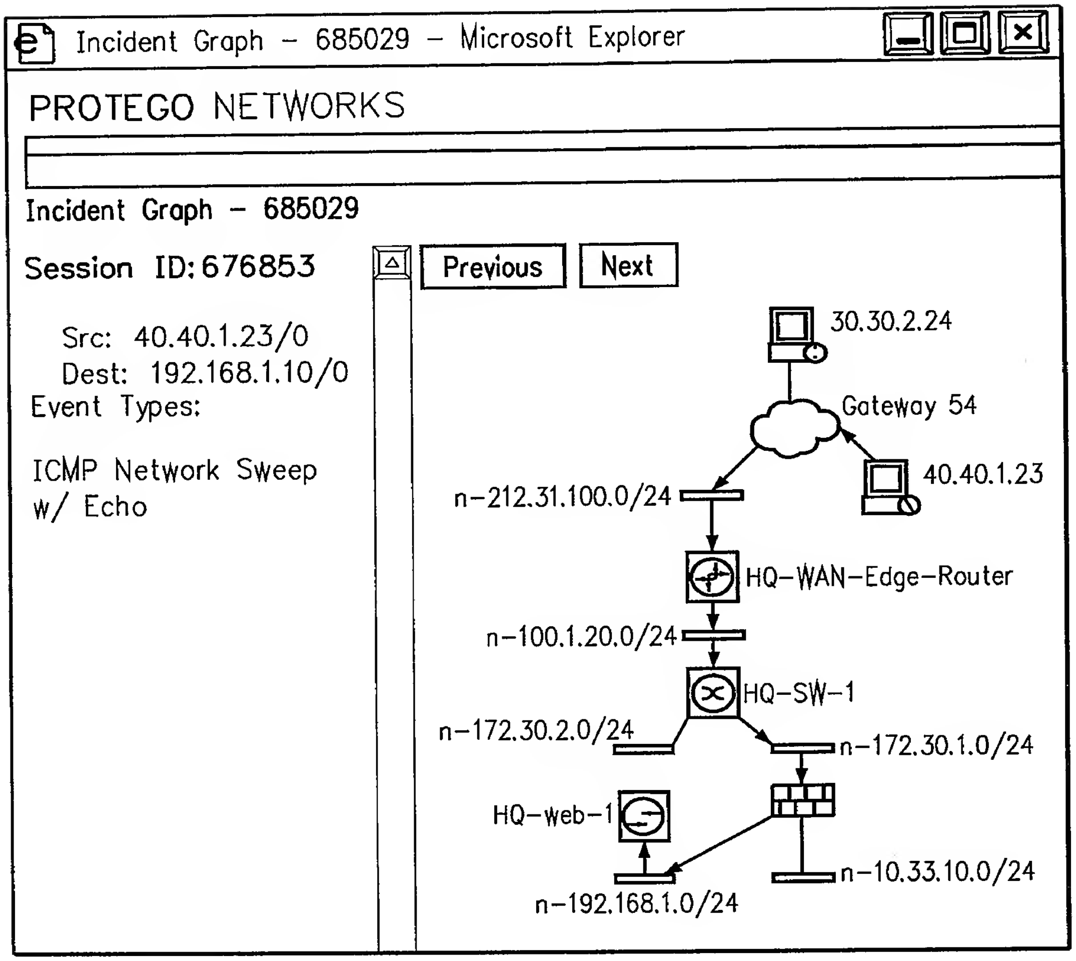
login: Administrator, Administrator (pnadmin) :: July 21, 2003 5:57:01 PM PDT ::

Raw Events

| Event/Session/ Incident ID | Reporting Device | Time | Raw Message |
|---|---|---|---|
| E:676853,<br>S:676853,<br>I:685029 ✉ | HQ-NIDS1 | Jul 21, 2003 5:26:42 PM PDT | 40.40.1.23/0 --> 192.168.1.10/0 ICMP ICMP Network Sweep w/Echo |

Protego Networks, Inc.

FIG. 12A



Incident Graph – 685029 – Microsoft Explorer

PROTEGO NETWORKS

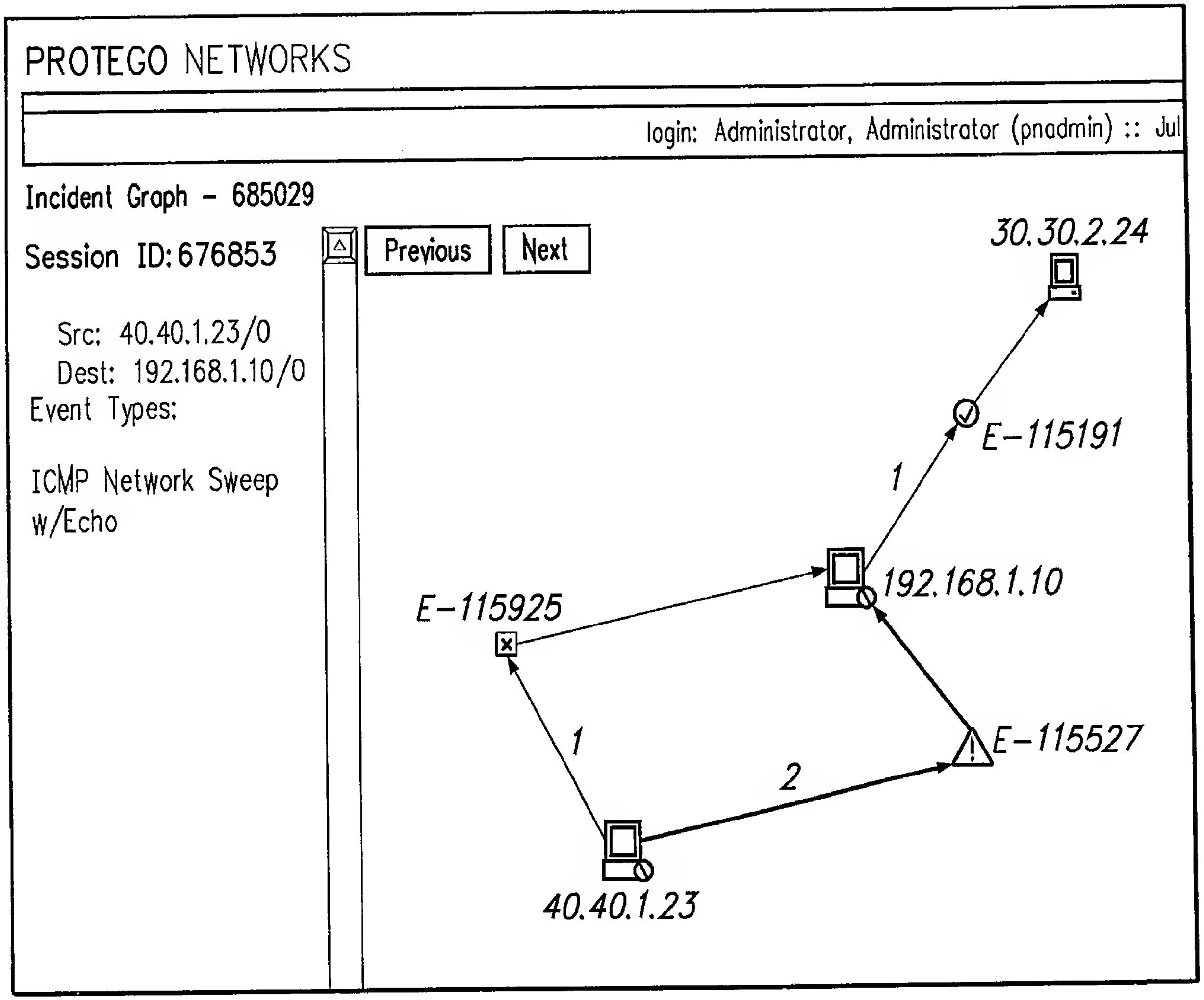
Incident Graph – 685029

Session ID: 676853

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/ Echo

FIG. 12B



PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul

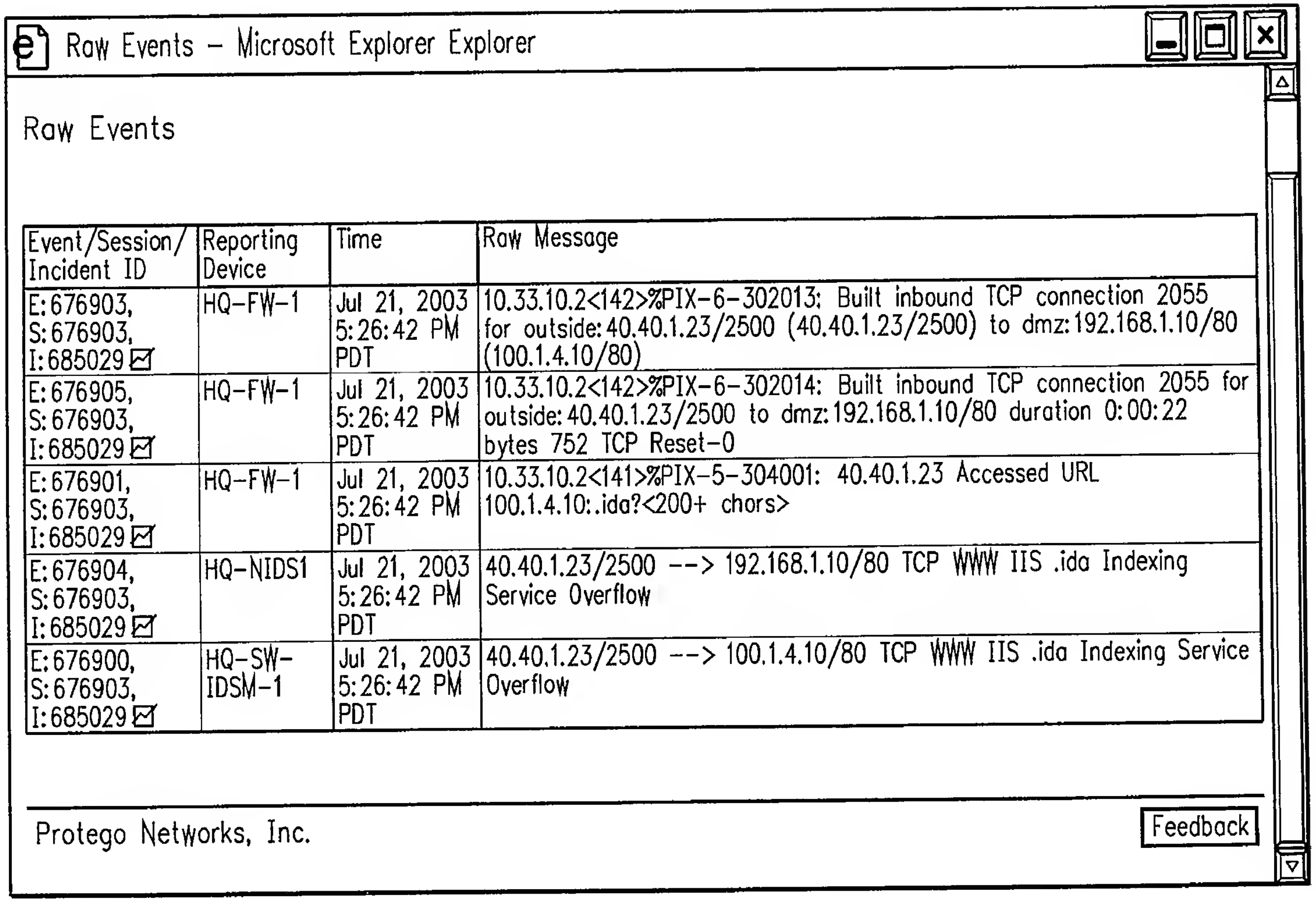
Incident Graph - 685029

Session ID: 676853

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/Echo

FIG. 12C

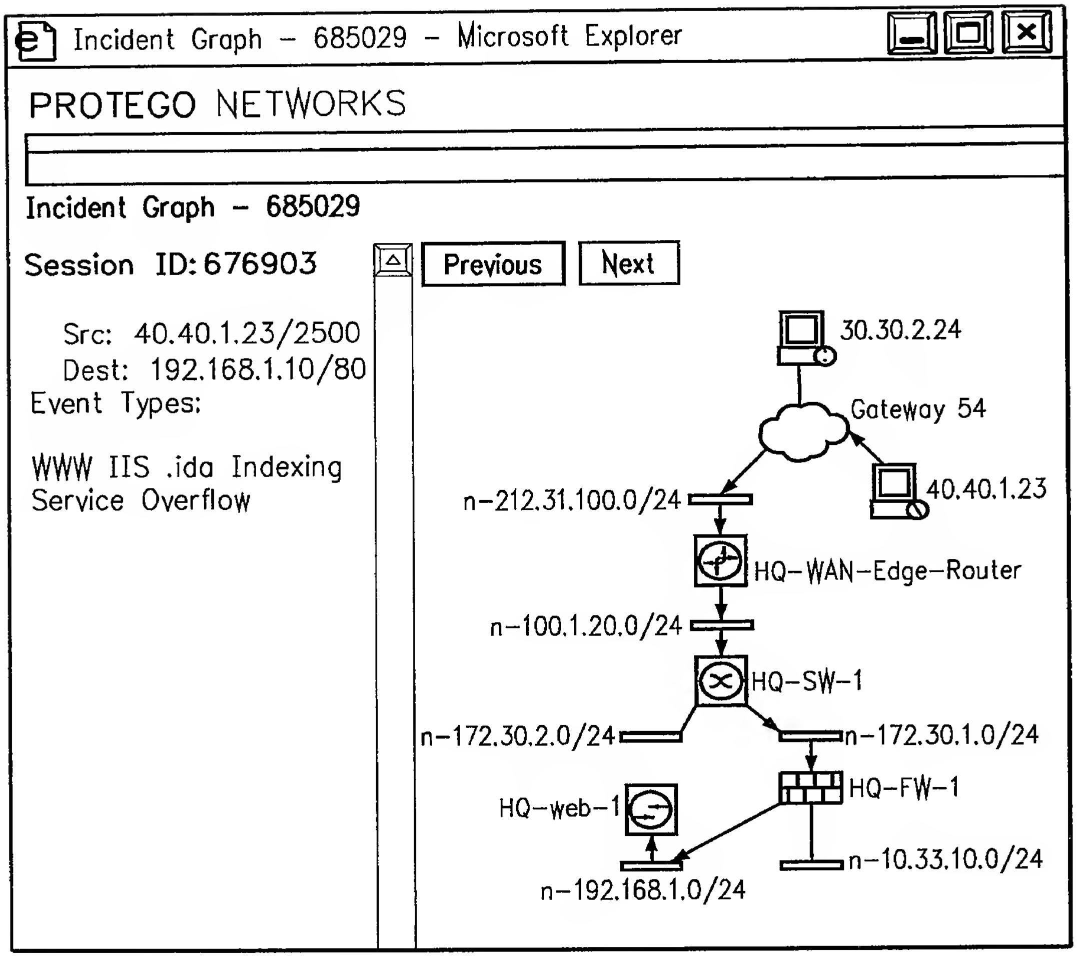


Raw Events

| Event/Session/ Incident ID | Reporting Device | Time | Raw Message |
|---|---|---|---|
| E:676903,<br>S:676903,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:42 PM PDT | 10.33.10.2<142>%PIX-6-302013: Built inbound TCP connection 2055 for outside:40.40.1.23/2500 (40.40.1.23/2500) to dmz:192.168.1.10/80 (100.1.4.10/80) |
| E:676905,<br>S:676903,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:42 PM PDT | 10.33.10.2<142>%PIX-6-302014: Built inbound TCP connection 2055 for outside:40.40.1.23/2500 to dmz:192.168.1.10/80 duration 0:00:22 bytes 752 TCP Reset-0 |
| E:676901,<br>S:676903,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:42 PM PDT | 10.33.10.2<141>%PIX-5-304001: 40.40.1.23 Accessed URL 100.1.4.10:.ida?<200+ chars> |
| E:676904,<br>S:676903,<br>I:685029 ☑ | HQ-NIDS1 | Jul 21, 2003 5:26:42 PM PDT | 40.40.1.23/2500 --> 192.168.1.10/80 TCP WWW IIS .ida Indexing Service Overflow |
| E:676900,<br>S:676903,<br>I:685029 ☑ | HQ-SW-IDSM-1 | Jul 21, 2003 5:26:42 PM PDT | 40.40.1.23/2500 --> 100.1.4.10/80 TCP WWW IIS .ida Indexing Service Overflow |

Protego Networks, Inc.

FIG. 13A



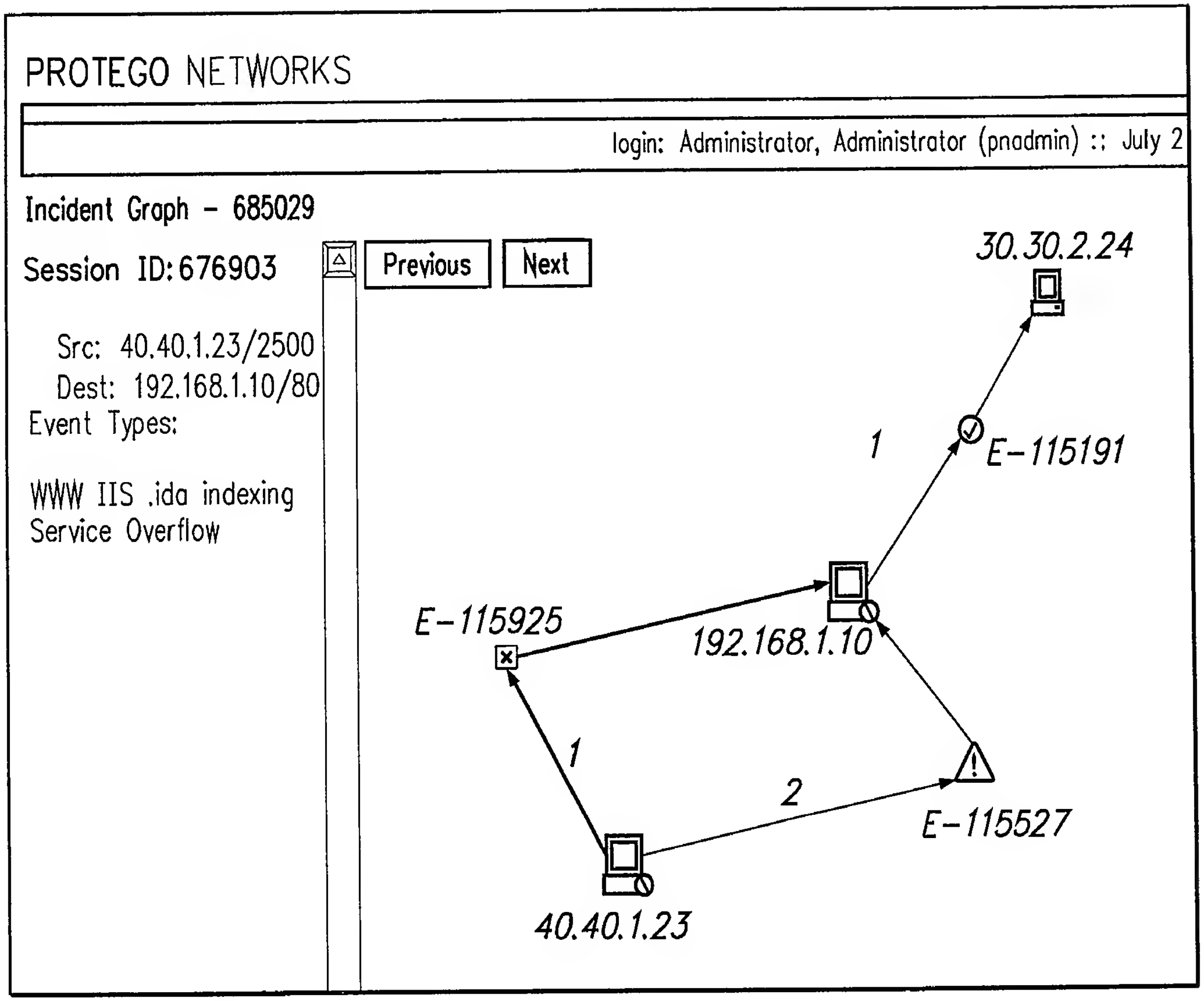
Incident Graph – 685029

Session ID: 676903

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida Indexing Service Overflow

*FIG. 13B*



PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: July 2

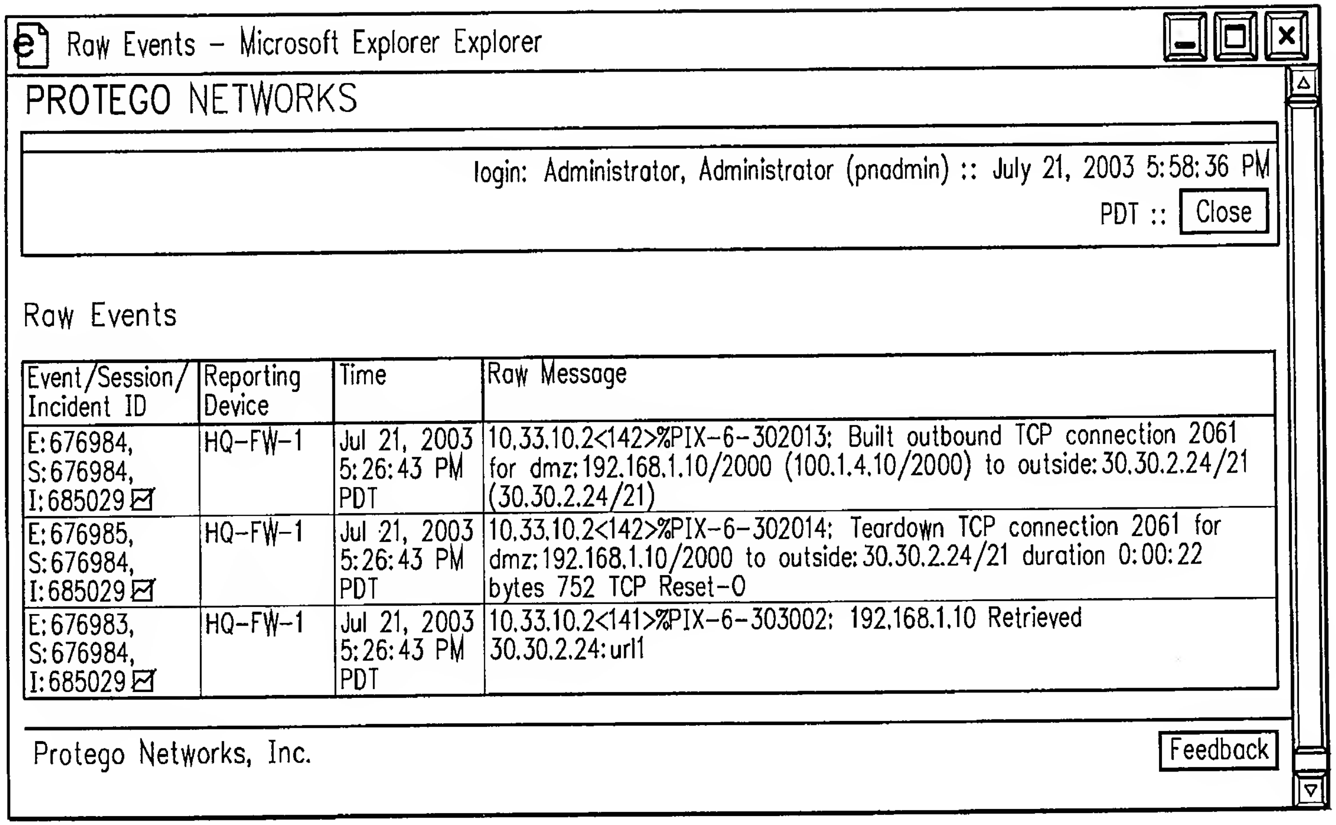
Incident Graph - 685029

Session ID:676903

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida indexing
Service Overflow

FIG. 13C

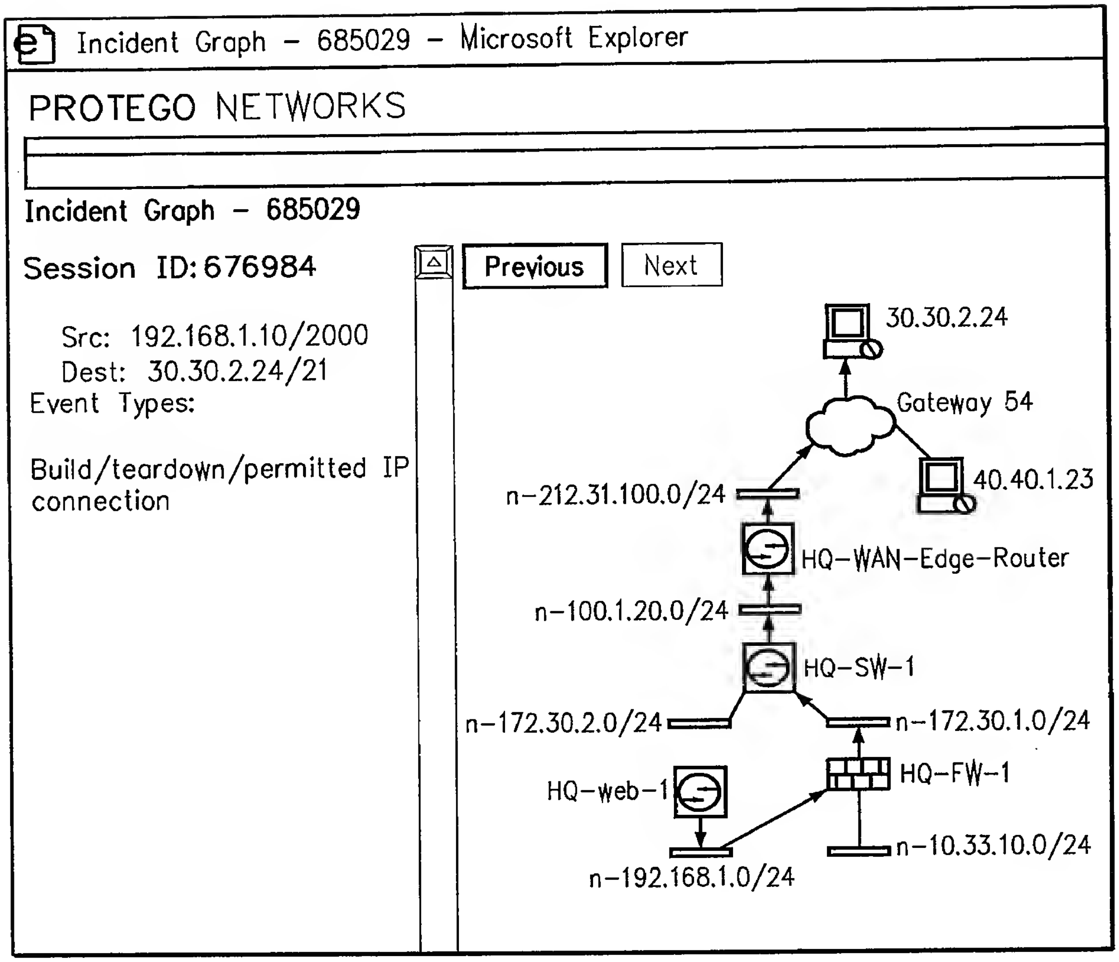


login: Administrator, Administrator (pnadmin) :: July 21, 2003 5:58:36 PM PDT ::

Raw Events

| Event/Session/ Incident ID | Reporting Device | Time | Raw Message |
|---|---|---|---|
| E:676984,<br>S:676984,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:43 PM PDT | 10.33.10.2<142>%PIX-6-302013: Built outbound TCP connection 2061 for dmz:192.168.1.10/2000 (100.1.4.10/2000) to outside:30.30.2.24/21 (30.30.2.24/21) |
| E:676985,<br>S:676984,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:43 PM PDT | 10.33.10.2<142>%PIX-6-302014: Teardown TCP connection 2061 for dmz:192.168.1.10/2000 to outside:30.30.2.24/21 duration 0:00:22 bytes 752 TCP Reset-O |
| E:676983,<br>S:676984,<br>I:685029 ☑ | HQ-FW-1 | Jul 21, 2003 5:26:43 PM PDT | 10.33.10.2<141>%PIX-6-303002: 192.168.1.10 Retrieved 30.30.2.24:url1 |

FIG. 14A



Incident Graph – 685029 – Microsoft Explorer

PROTEGO NETWORKS

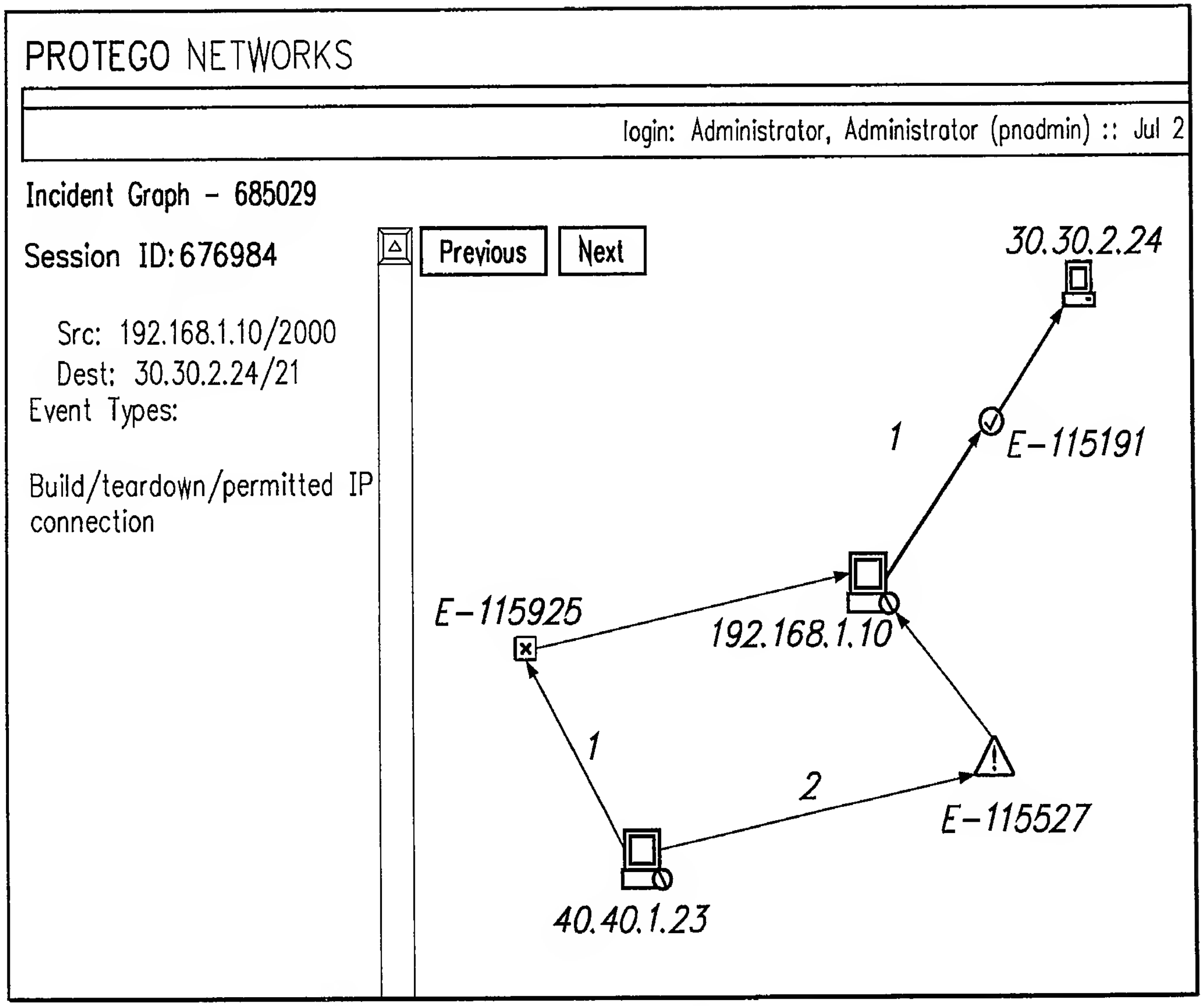
Incident Graph – 685029

Session ID: 676984

Src: 192.168.1.10/2000
Dest: 30.30.2.24/21
Event Types:

Build/teardown/permitted IP connection

FIG. 14B



PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 2

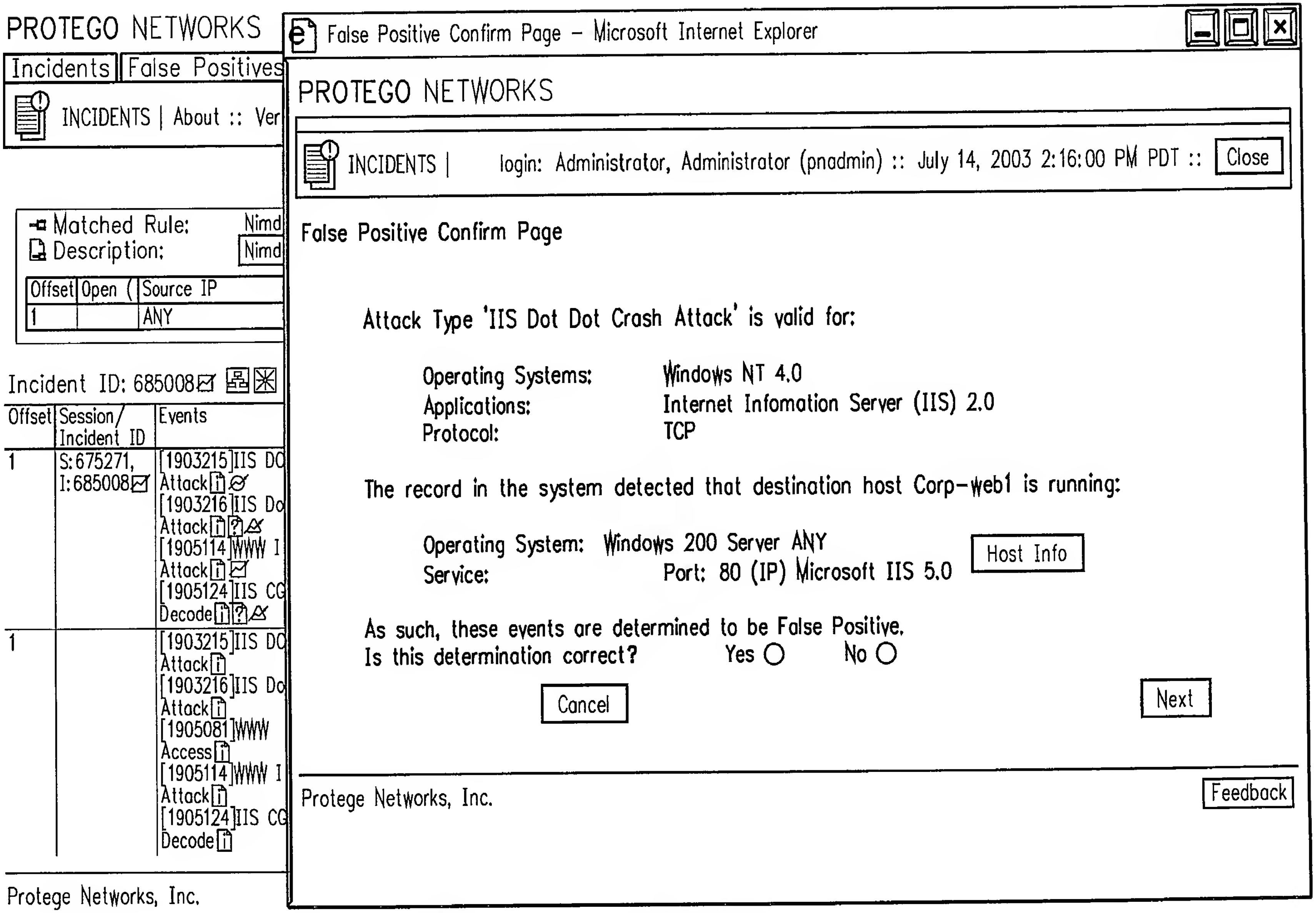
Incident Graph - 685029

Session ID:676984

Src: 192.168.1.10/2000
Dest: 30.30.2.24/21
Event Types:

Build/teardown/permitted IP connection

FIG. 14C



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Ver

Matched Rule: Nimd
Description: Nimd

| Offset | Open ( | Source IP |
|---|---|---|
| 1 | | ANY |

Incident ID: 685008

| Offset | Session/ Incident ID | Events |
|---|---|---|
| 1 | S:675271, I:685008 | [1903215]IIS DO Attack<br>[1903216]IIS Do Attack<br>[1905114]WWW I Attack<br>[1905124]IIS CG Decode |
| 1 | | [1903215]IIS DO Attack<br>[1903216]IIS Do Attack<br>[1905081]WWW Access<br>[1905114]WWW I Attack<br>[1905124]IIS CG Decode |

Protege Networks, Inc.

False Positive Confirm Page – Microsoft Internet Explorer

PROTEGO NETWORKS

INCIDENTS | login: Administrator, Administrator (pnadmin) :: July 14, 2003 2:16:00 PM PDT :: Close

False Positive Confirm Page

Attack Type 'IIS Dot Dot Crash Attack' is valid for:

Operating Systems: Windows NT 4.0
Applications: Internet Infomation Server (IIS) 2.0
Protocol: TCP

The record in the system detected that destination host Corp-web1 is running:

Operating System: Windows 200 Server ANY
Service: Port: 80 (IP) Microsoft IIS 5.0

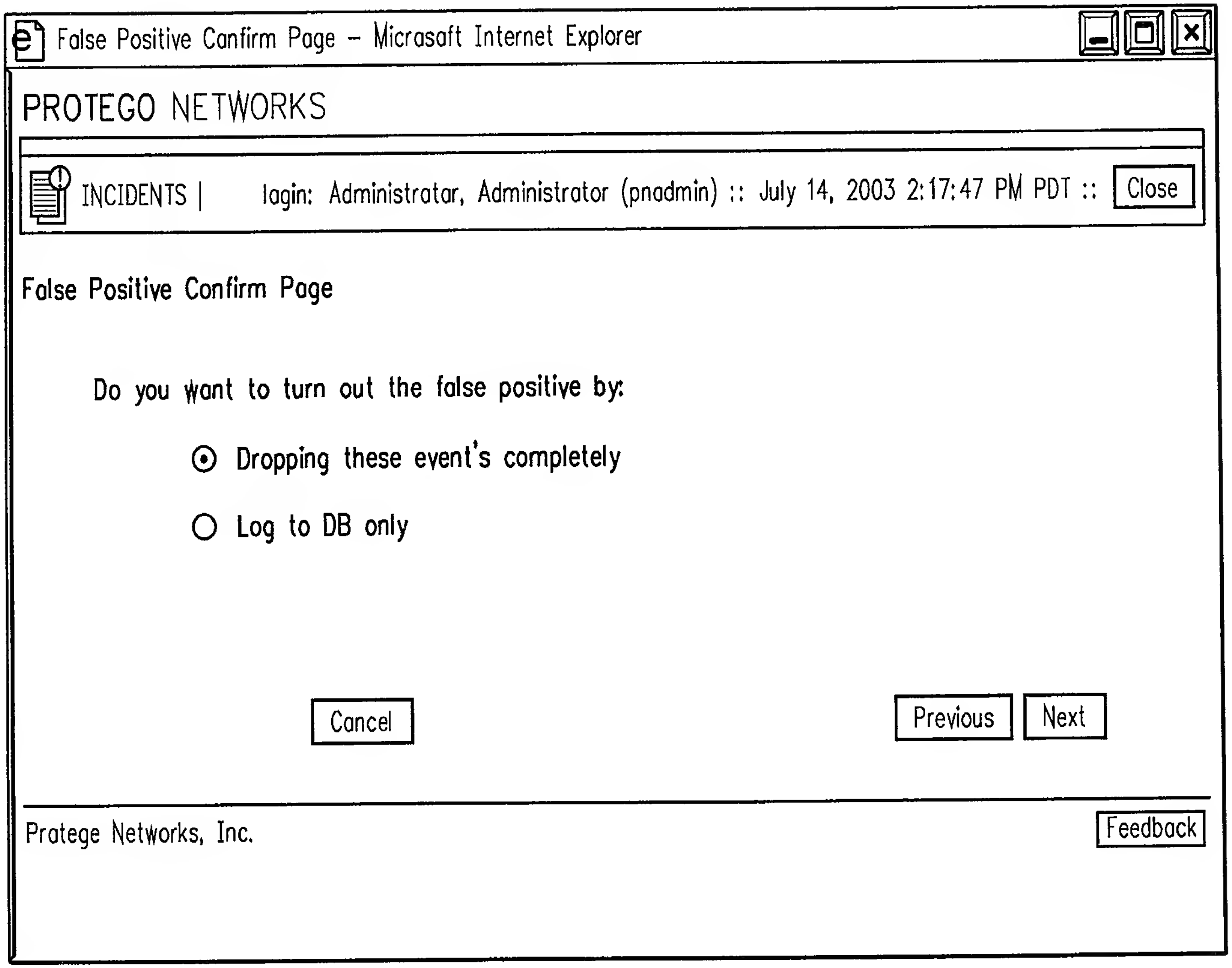
Host Info

As such, these events are determined to be False Positive.
Is this determination correct? Yes ○ No ○

Cancel Next

Protege Networks, Inc. Feedback

FIG. 15A



False Positive Confirm Page – Micrasaft Internet Explorer

PROTEGO NETWORKS

INCIDENTS | lagin: Administratar, Administrator (pnadmin) :: July 14, 2003 2:17:47 PM PDT ::

False Positive Confirm Page

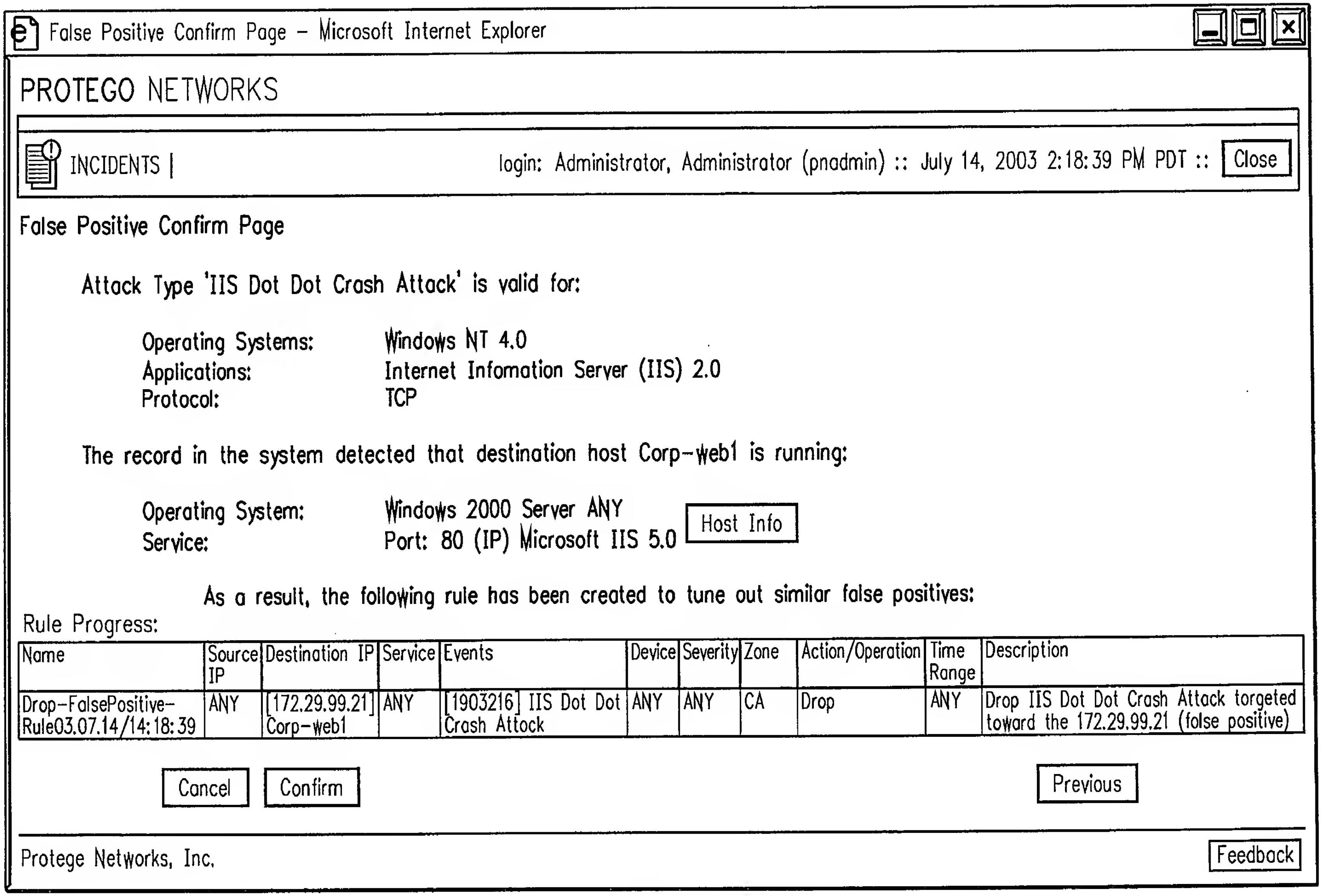
Do you want to turn out the false positive by:

⦿ Dropping these event's completely

○ Log to DB only

Pratege Networks, Inc.

FIG. 15B



login: Administrator, Administrator (pnadmin) :: July 14, 2003 2:18:39 PM PDT ::

False Positive Confirm Page

Attack Type 'IIS Dot Dot Crash Attack' is valid for:

| | |
|---|---|
| Operating Systems: | Windows NT 4.0 |
| Applications: | Internet Infomation Server (IIS) 2.0 |
| Protocol: | TCP |

The record in the system detected that destination host Corp-web1 is running:

| | |
|---|---|
| Operating System: | Windows 2000 Server ANY |
| Service: | Port: 80 (IP) Microsoft IIS 5.0 |

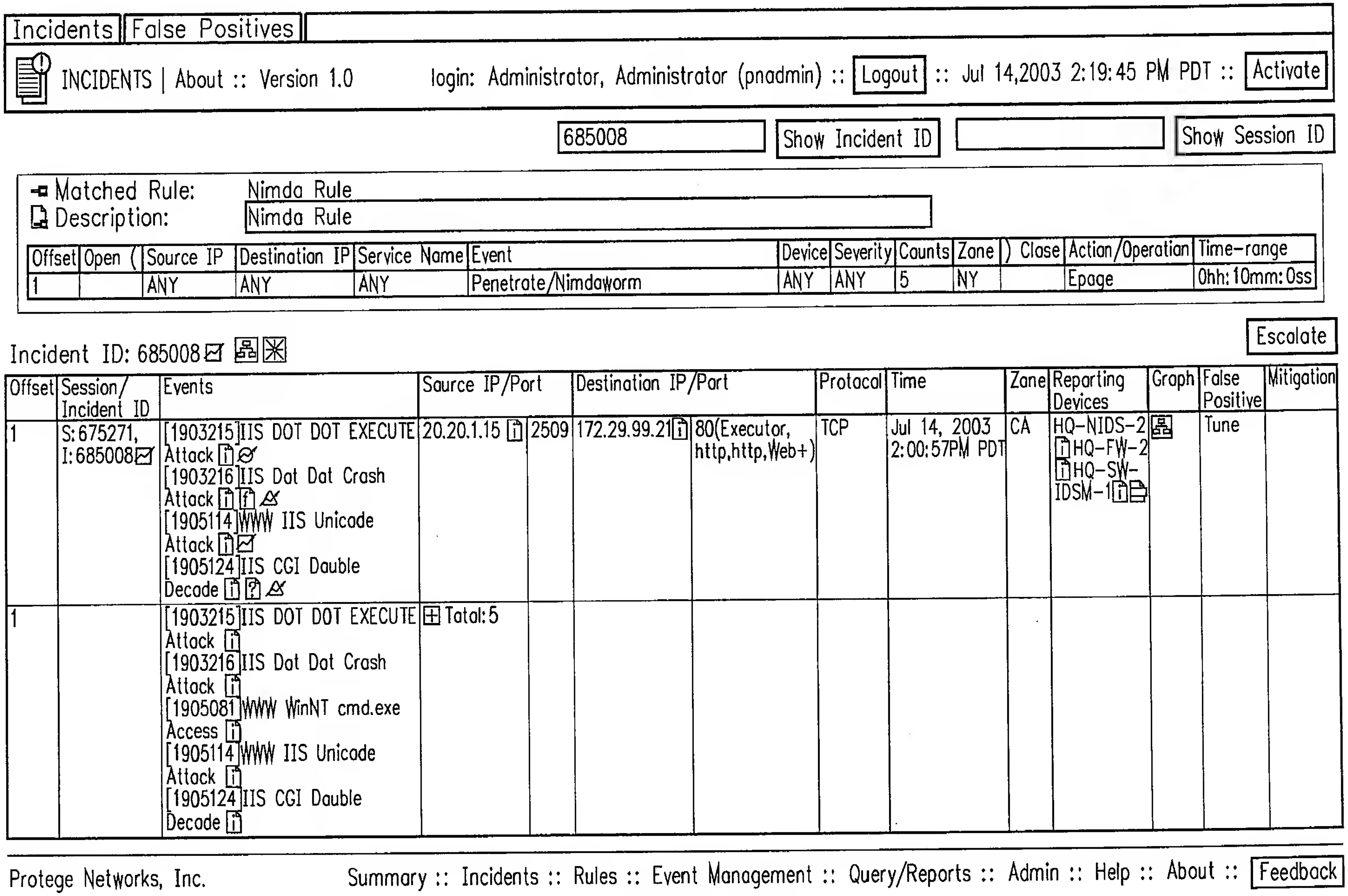
As a result, the following rule has been created to tune out similar false positives:

Rule Progress:

| Name | Source IP | Destination IP | Service | Events | Device | Severity | Zone | Action/Operation | Time Range | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| Drop-FalsePositive-Rule03.07.14/14:18:39 | ANY | [172.29.99.21] Corp-web1 | ANY | [1903216] IIS Dot Dot Crash Attack | ANY | ANY | CA | Drop | ANY | Drop IIS Dot Dot Crash Attack torgeted toward the 172.29.99.21 (false positive) |

Protege Networks, Inc.

FIG. 15C



Incidents | False Positives

INCIDENTS | About :: Version 1.0 login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14,2003 2:19:45 PM PDT :: Activate

685008 Show Incident ID Show Session ID

Matched Rule: Nimda Rule
Description: Nimda Rule

| Offset | Open ( | Source IP | Destination IP | Service Name | Event | Device | Severity | Counts | Zone | ) Close | Action/Operation | Time-range |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | ANY | ANY | ANY | Penetrate/Nimdaworm | ANY | ANY | 5 | NY | | Epage | 0hh:10mm:0ss |

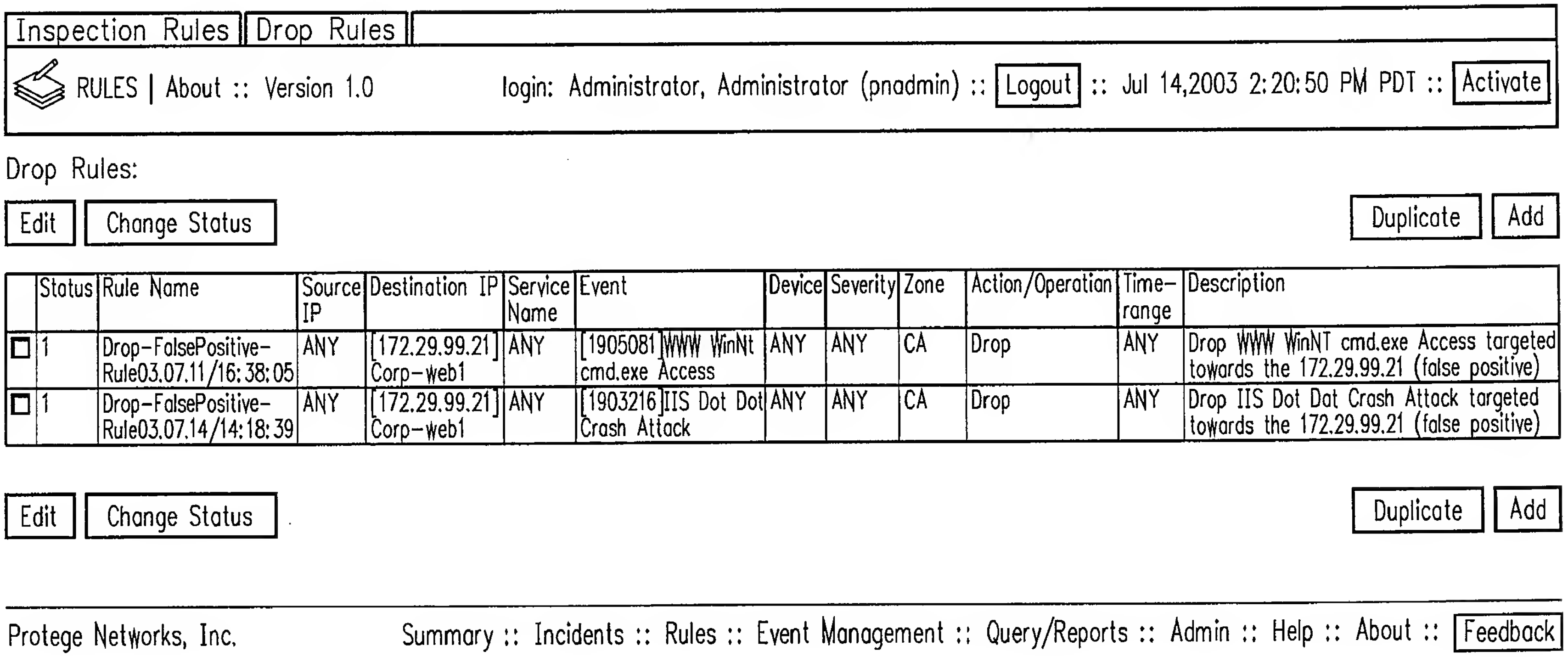
Escalate

Incident ID: 685008 ☑

| Offset | Session/ Incident ID | Events | Saurce IP/Port | | Destination IP/Part | | Protocal | Time | Zone | Reporting Devices | Graph | False Positive | Mitigation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | S:675271, I:685008 ☑ | [1903215]IIS DOT DOT EXECUTE Attack ⓘ<br>[1903216]IIS Dot Dot Crash Attack ⓘ<br>[1905114]WWW IIS Unicode Attack ⓘ ☑<br>[1905124]IIS CGI Dauble Decade ⓘ | 20.20.1.15 ⓘ | 2509 | 172.29.99.21 ⓘ | 80(Executor, http,http,Web+) | TCP | Jul 14, 2003 2:00:57PM PDT | CA | HQ-NIDS-2<br>HQ-FW-2<br>HQ-SW-IDSM-1 | | Tune | |
| 1 | | [1903215]IIS DOT DOT EXECUTE Attack ⓘ<br>[1903216]IIS Dot Dot Crash Attack ⓘ<br>[1905081]WWW WinNT cmd.exe Access ⓘ<br>[1905114]WWW IIS Unicode Attack ⓘ<br>[1905124]IIS CGI Dauble Decade ⓘ | ⊞ Tatal:5 | | | | | | | | | | |

Protege Networks, Inc. Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 15D



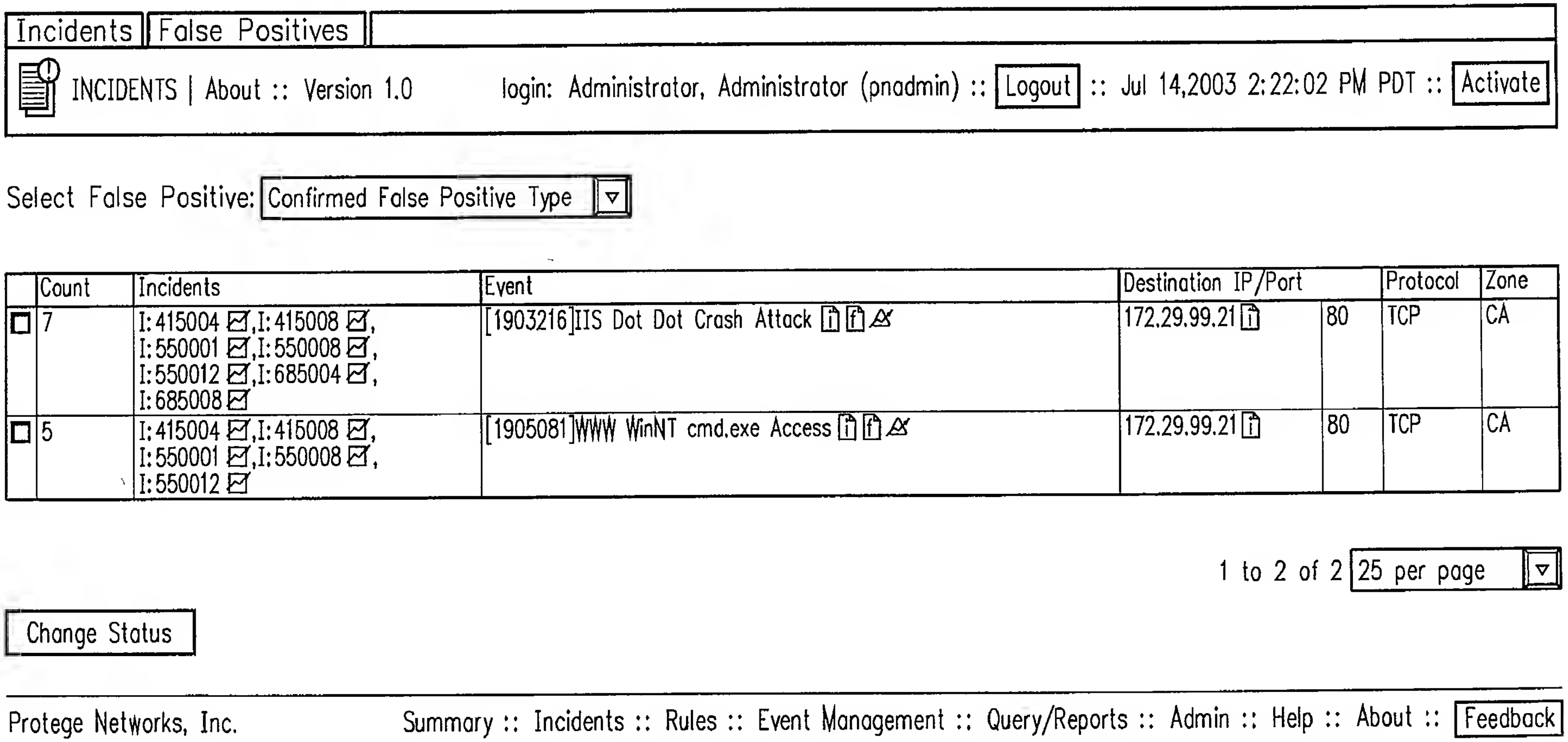
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14,2003 2:20:50 PM PDT :: Activate

Drop Rules:

|  | Status | Rule Name | Source IP | Destination IP | Service Name | Event | Device | Severity | Zone | Action/Operation | Time-range | Description |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Drop-FalsePositive-Rule03.07.11/16:38:05 | ANY | [172.29.99.21] Corp-web1 | ANY | [1905081]WWW WinNt cmd.exe Access | ANY | ANY | CA | Drop | ANY | Drop WWW WinNT cmd.exe Access targeted towards the 172.29.99.21 (false positive) |
| □ | 1 | Drop-FalsePositive-Rule03.07.14/14:18:39 | ANY | [172.29.99.21] Corp-web1 | ANY | [1903216]IIS Dot Dot Crash Attack | ANY | ANY | CA | Drop | ANY | Drop IIS Dot Dot Crash Attack targeted towards the 172.29.99.21 (false positive) |

Edit
Change Status
Duplicate
Add
Protege Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 16A



INCIDENTS | About :: Version 1.0 login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14,2003 2:22:02 PM PDT :: Activate

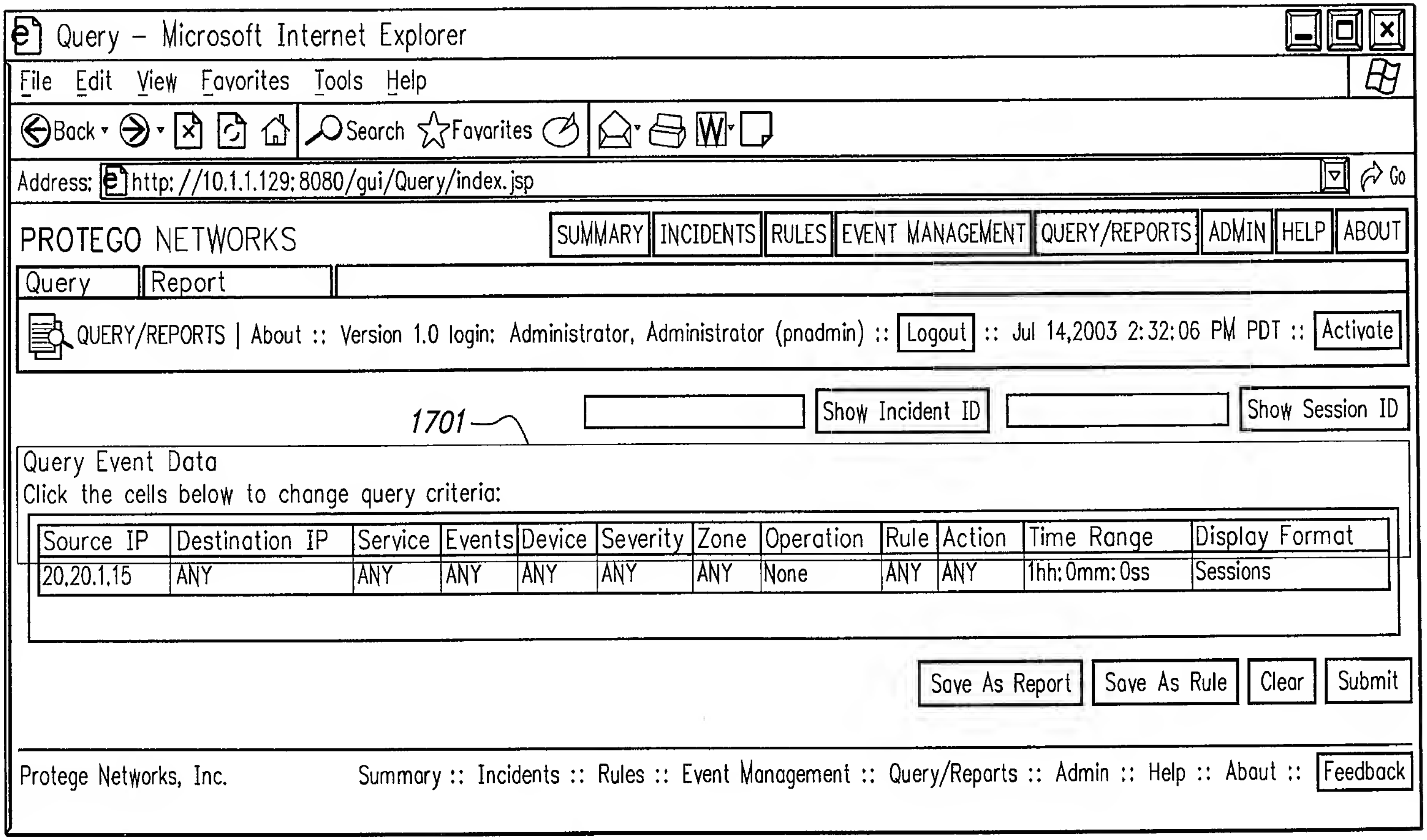
Select False Positive: Confirmed False Positive Type ▽

| | Count | Incidents | Event | Destination IP/Port | | Protocol | Zone |
|---|---|---|---|---|---|---|---|
| □ | 7 | I:415004 ☑,I:415008 ☑,<br>I:550001 ☑,I:550008 ☑,<br>I:550012 ☑,I:685004 ☑,<br>I:685008 ☑ | [1903216]IIS Dot Dot Crash Attack | 172.29.99.21 | 80 | TCP | CA |
| □ | 5 | I:415004 ☑,I:415008 ☑,<br>I:550001 ☑,I:550008 ☑,<br>I:550012 ☑ | [1905081]WWW WinNT cmd.exe Access | 172.29.99.21 | 80 | TCP | CA |

1 to 2 of 2 25 per page ▽

Protege Networks, Inc. Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 16B



Address: http://10.1.1.129:8080/gui/Query/index.jsp

QUERY/REPORTS | About :: Version 1.0 login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14,2003 2:32:06 PM PDT :: Activate

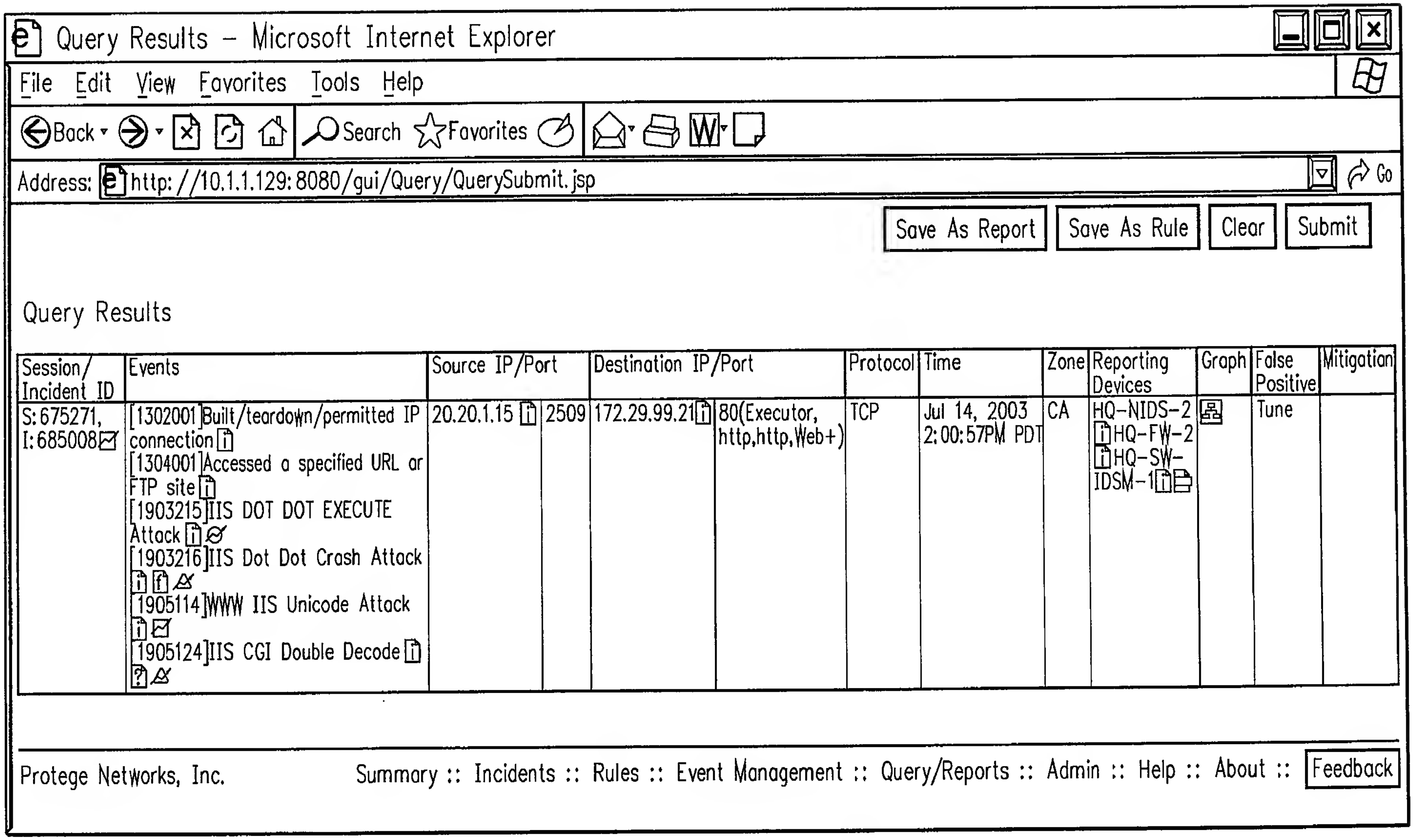
Query Event Data

Click the cells below to change query criteria:

| Source IP | Destination IP | Service | Events | Device | Severity | Zone | Operation | Rule | Action | Time Range | Display Format |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 20.20.1.15 | ANY | ANY | ANY | ANY | ANY | ANY | None | ANY | ANY | 1hh:0mm:0ss | Sessions |

Protege Networks, Inc. Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About :: Feedback

FIG. 17A

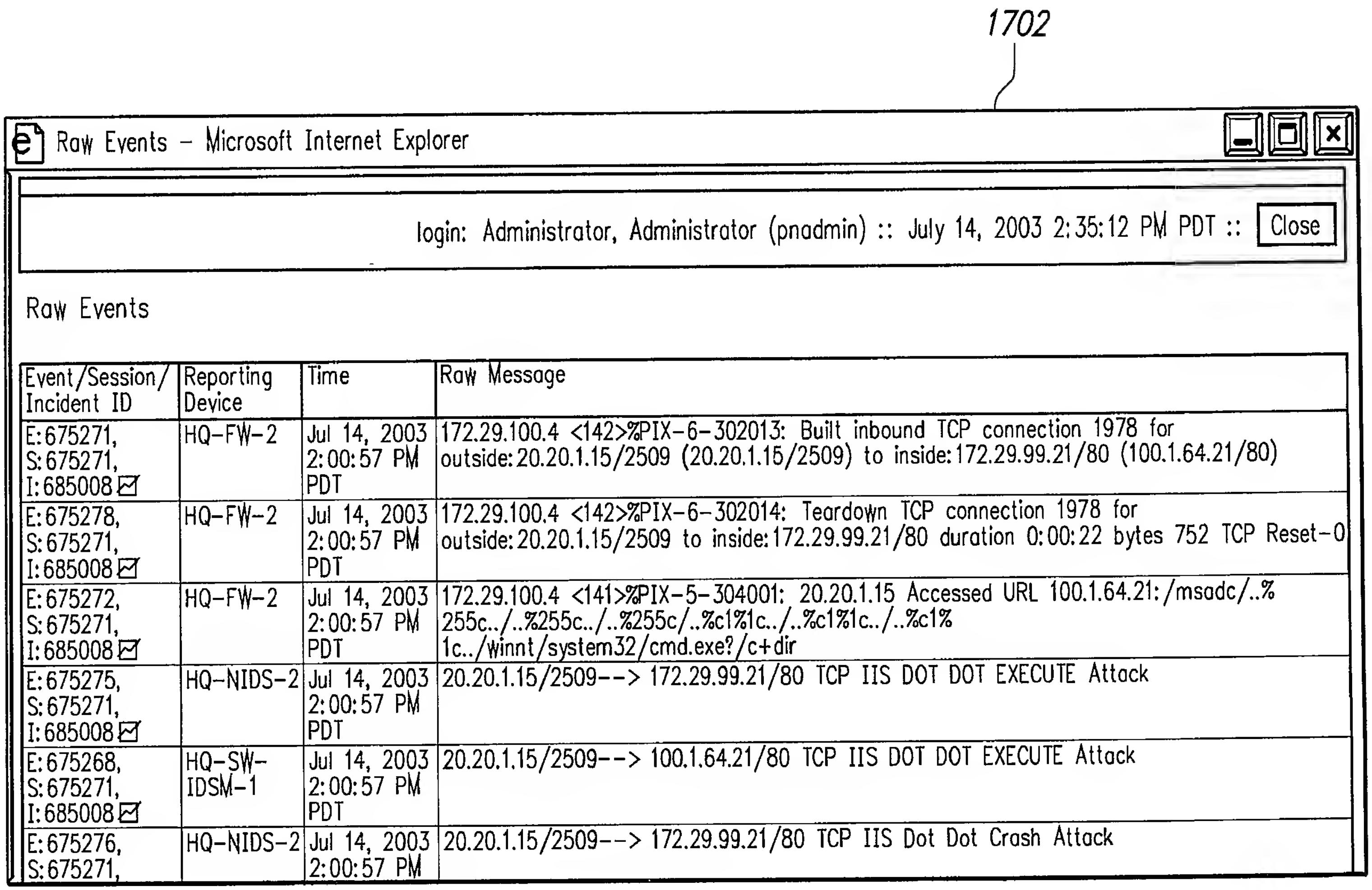

Query Results – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address: http://10.1.1.129:8080/gui/Query/QuerySubmit.jsp
Go
Save As Report
Save As Rule
Clear
Submit

Query Results

| Session/ Incident ID | Events | Source IP/Port | | Destination IP/Port | | Protocol | Time | Zone | Reporting Devices | Graph | False Positive | Mitigation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S:675271,<br>I:685008 | [1302001]Built/teardown/permitted IP connection<br>[1304001]Accessed a specified URL or FTP site<br>[1903215]IIS DOT DOT EXECUTE Attack<br>[1903216]IIS Dot Dot Crash Attack<br>[1905114]WWW IIS Unicode Attack<br>[1905124]IIS CGI Double Decode | 20.20.1.15 | 2509 | 172.29.99.21 | 80(Executor, http,http,Web+) | TCP | Jul 14, 2003 2:00:57PM PDT | CA | HQ-NIDS-2<br>HQ-FW-2<br>HQ-SW-IDSM-1 | | Tune | |

Protege Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query/Reports :: Admin :: Help :: About ::
Feedback

FIG. 17B



login: Administrator, Administrator (pnadmin) :: July 14, 2003 2:35:12 PM PDT ::

Raw Events

| Event/Session/ Incident ID | Reporting Device | Time | Raw Message |
|---|---|---|---|
| E:675271,<br>S:675271,<br>I:685008 ☑ | HQ-FW-2 | Jul 14, 2003 2:00:57 PM PDT | 172.29.100.4 <142>%PIX-6-302013: Built inbound TCP connection 1978 for outside:20.20.1.15/2509 (20.20.1.15/2509) to inside:172.29.99.21/80 (100.1.64.21/80) |
| E:675278,<br>S:675271,<br>I:685008 ☑ | HQ-FW-2 | Jul 14, 2003 2:00:57 PM PDT | 172.29.100.4 <142>%PIX-6-302014: Teardown TCP connection 1978 for outside:20.20.1.15/2509 to inside:172.29.99.21/80 duration 0:00:22 bytes 752 TCP Reset-O |
| E:675272,<br>S:675271,<br>I:685008 ☑ | HQ-FW-2 | Jul 14, 2003 2:00:57 PM PDT | 172.29.100.4 <141>%PIX-5-304001: 20.20.1.15 Accessed URL 100.1.64.21:/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir |
| E:675275,<br>S:675271,<br>I:685008 ☑ | HQ-NIDS-2 | Jul 14, 2003 2:00:57 PM PDT | 20.20.1.15/2509--> 172.29.99.21/80 TCP IIS DOT DOT EXECUTE Attack |
| E:675268,<br>S:675271,<br>I:685008 ☑ | HQ-SW-IDSM-1 | Jul 14, 2003 2:00:57 PM PDT | 20.20.1.15/2509--> 100.1.64.21/80 TCP IIS DOT DOT EXECUTE Attack |
| E:675276,<br>S:675271, | HQ-NIDS-2 | Jul 14, 2003 2:00:57 PM | 20.20.1.15/2509--> 172.29.99.21/80 TCP IIS Dot Dot Crash Attack |

FIG. 17C